



**Intelligent Transport Systems (ITS);  
Testing;  
Conformance test specifications for ITS Security;  
Part 2: Test Suite Structure and Test Purposes (TSS & TP)**

---

**Reference**

RTS/ITS-005104

---

**Keywords**

ITS, security, testing, TSS&amp;TP

**ETSI**

---

650 Route des Lucioles  
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B  
Association à but non lucratif enregistrée à la  
Sous-Préfecture de Grasse (06) N° w061004871

---

**Important notice**

The present document can be downloaded from:

<http://www.etsi.org/standards-search>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at [www.etsi.org/deliver](http://www.etsi.org/deliver).

Users of the present document should be aware that the document may be subject to revision or change of status.

Information on the current status of this and other ETSI documents is available at

<https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

If you find errors in the present document, please send your comment to one of the following services:

<https://portal.etsi.org/People/CommitteeSupportStaff.aspx>

If you find a security vulnerability in the present document, please report it through our  
Coordinated Vulnerability Disclosure Program:

<https://www.etsi.org/standards/coordinated-vulnerability-disclosure>

---

**Notice of disclaimer & limitation of liability**

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.

No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

---

**Copyright Notification**

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2022.  
All rights reserved.

# Contents

Intellectual Property Rights .....	5
Foreword.....	5
Modal verbs terminology.....	5
1 Scope .....	6
2 References .....	6
2.1 Normative references .....	6
2.2 Informative references.....	6
3 Definition of terms, symbols and abbreviations.....	7
3.1 Terms.....	7
3.2 Symbols.....	7
3.3 Abbreviations .....	7
4 Test Suite Structure (TSS).....	8
4.1 Structure for Security tests .....	8
5 Test Purposes (TP) .....	8
5.1 Introduction .....	8
5.1.1 TP definition conventions.....	8
5.1.2 TP Identifier naming conventions.....	8
5.1.3 Rules for the behaviour description .....	9
5.1.4 Sources of TP definitions.....	9
5.1.5 Mnemonics for PICS reference.....	9
6 ITS-S Security .....	10
6.1 Overview .....	10
6.1.1 Certificates content .....	10
6.1.1.1 Root Certificate Authorities certificates.....	10
6.1.1.2 Authorization Authorities certificates .....	11
6.1.1.3 Authorization Tickets.....	12
6.2 Sending behaviour .....	13
6.2.1 General sending behaviour .....	13
6.2.1.1 Check the message protocol version .....	13
6.2.2 CAM profile.....	14
6.2.2.1 Check that secured CAM is signed .....	14
6.2.2.2 Check secured CAM AID value.....	14
6.2.2.3 Check header fields .....	15
6.2.2.4 Check signer information.....	15
6.2.2.5 Check that IUT sends certificate to unknown ITS-S.....	17
6.2.2.6 Check that IUT restarts the timer when the certificate has been sent.....	18
6.2.2.7 Check sending certificate request for unknown certificate .....	18
6.2.2.8 Check that IUT sends AT certificate when requested .....	20
6.2.2.9 Check that IUT sends AA certificate when requested.....	21
6.2.2.10 Check generation time.....	25
6.2.2.11 Check payload.....	25
6.2.2.12 Check signing permissions.....	26
6.2.2.13 Check signature.....	26
6.2.2.14 Check support for certificate content .....	27
6.2.2.15 Check certificate consistency conditions .....	28
6.2.3 DENM profile.....	30
6.2.3.1 Check secured DENM is signed.....	30
6.2.3.2 Check secured DENM AID value .....	30
6.2.3.3 Check header fields .....	31
6.2.3.4 Check signer information.....	31
6.2.3.5 Check generation time.....	32
6.2.3.6 Check generation location.....	32
6.2.3.7 Check payload.....	34

6.2.3.8	Check signing permissions.....	35
6.2.3.9	Check signature.....	35
6.2.3.10	Check support for certificate content .....	36
6.2.3.11	Check certificate consistency conditions .....	37
6.2.4	Generic signed message profile .....	39
6.2.4.1	Check that secured message is signed.....	39
6.2.4.2	Check secured AID value.....	39
6.2.4.3	Check header field.....	40
6.2.4.4	Check that signer info is a certificate or digest .....	40
6.2.4.5	Check generation time.....	41
6.2.4.6	Check payload.....	41
6.2.4.7	Check signing permissions.....	42
6.2.4.8	Check signature.....	42
6.3	Receiving behaviour.....	43
6.3.1	Check the message protocol version.....	43
6.3.2	CAM profile.....	44
6.3.2.1	Check the valid message receiving .....	44
6.3.2.2	Check invalid HeaderInfo elements .....	47
6.3.2.3	Check invalid Signature elements .....	49
6.3.3	DENM profile.....	50
6.3.3.1	Check the valid message receiving .....	50
6.3.3.2	Check invalid HeaderInfo elements .....	53
6.3.3.3	Check invalid Signature elements .....	55
<b>Annex A (informative): Bibliography.....</b>		<b>56</b>
History .....		57

---

# Intellectual Property Rights

## Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: "*Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards*", which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<https://ipr.etsi.org/>).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

## Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

**DECT™**, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

---

# Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Intelligent Transport Systems (ITS).

The present document is part 2 of a multi-part deliverable. Full details of the entire series can be found in part 1 [3].

---

# Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

---

# 1 Scope

The present document provides the Test Suite Structure and Test Purposes (TSS & TP) for Security as defined in ETSI TS 103 097 [1] in accordance with the relevant guidance given in ISO/IEC 9646-7 [i.6].

The ISO standards for the methodology of conformance testing (ISO/IEC 9646-1 [i.3] and ISO/IEC 9646-2 [i.4]) as well as the ETSI rules for conformance testing (ETSI ETS 300 406 [i.7]) are used as a basis for the test methodology.

---

## 2 References

### 2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at <https://docbox.etsi.org/Reference/>.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

- [1] ETSI TS 103 097 (V1.4.1): "Intelligent Transport Systems (ITS); Security; Security header and certificate formats".
- [2] IEEE Std 1609.2™-2016: "IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages", as amended by IEEE Std 1609.2a™-2017: " IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages - Amendment 1".
- [3] ETSI TS 103 096-1 (V1.5.2): "Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 1: Protocol Implementation Conformance Statement (PICS)".
- [4] ETSI TS 102 871-1 (V1.4.1): "Intelligent Transport Systems (ITS); Testing; Conformance test specifications for GeoNetworking ITS-G5; Part 1: Test requirements and Protocol Implementation Conformance Statement (PICS) pro forma".
- [5] Void.

### 2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

- [i.1] ETSI EG 202 798 (V1.1.1): "Intelligent Transport Systems (ITS); Testing; Framework for conformance and interoperability testing".
- [i.2] ETSI TS 102 965 (V1.3.1): "Intelligent Transport Systems (ITS); Application Object Identifier (ITS-AID); Registration".

- [i.3] ISO/IEC 9646-1 (1994): "Information technology -- Open Systems Interconnection -- Conformance testing methodology and framework -- Part 1: General concepts".
- [i.4] ISO/IEC 9646-2 (1994): "Information technology -- Open Systems Interconnection -- Conformance testing methodology and framework -- Part 2: Abstract Test Suite specification".
- [i.5] ISO/IEC 9646-6 (1994): "Information technology -- Open Systems Interconnection -- Conformance testing methodology and framework -- Part 6: Protocol profile test specification".
- [i.6] ISO/IEC 9646-7 (1995): "Information technology -- Open Systems Interconnection -- Conformance testing methodology and framework -- Part 7: Implementation Conformance Statements".
- [i.7] ETSI ETS 300 406 (1995): "Methods for testing and Specification (MTS); Protocol and profile conformance testing specifications; Standardization methodology".

---

## 3 Definition of terms, symbols and abbreviations

### 3.1 Terms

For the purposes of the present document, the terms given in ETSI TS 103 097 [1], ETSI TS 102 965 [i.2], ISO/IEC 9646-6 [i.5] and ISO/IEC 9646-7 [i.6] apply.

### 3.2 Symbols

Void.

### 3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AA	Authorization Authority
AID	Application Identifier
AID_CAM	ITS Application Identifier for CAM
AID_DENM	Application Identifier for DENM
AID_GN	Application Identifier for general GeoNetworking messages
AT	Authorization Ticket
ATS	Abstract Test Suite
BO	Exceptional Behaviour
BV	Valid Behaviour
CA	Certificate Authority
CAM	Co-operative Awareness Messages
CAN	Controller Area Network
CERT	Certificate
DE	Data Element
DEN	Decentralized Environmental Notification
DENM	Decentralized Environmental Notification Message
EA	Enrolment Authority
ECC	Elliptic Curve Cryptography
GN	GeoNetworking
ITS	Intelligent Transport Systems
ITS-S	Intelligent Transport System - Station
IUT	Implementation under Test
MSG	Message
PICS	Protocol Implementation Conformance Statement
PSID	Provider Service Identifier
RCA	Root Certificate Authority
SSP	Service Specific Permissions

TP Test Purposes  
TSS Test Suite Structure

## 4 Test Suite Structure (TSS)

### 4.1 Structure for Security tests

Table 1 shows the Security Test Suite Structure (TSS) defined for conformance testing.

**Table 1: TSS for Security**

Root	Group	Category
Security	ITS-S data transfer	Valid
	ITS-S - AA authorization	Valid
	ITS-S - EA enrolment	Valid
	Sending behaviour	Valid
	Receiving behaviour	Valid and Invalid
	Generic messages	Valid
	CAM testing	Valid
	DENM testing	Valid
	Certificate testing	Valid

## 5 Test Purposes (TP)

### 5.1 Introduction

#### 5.1.1 TP definition conventions

The TP definition is built according to ETSI EG 202 798 [i.1].

#### 5.1.2 TP Identifier naming conventions

The identifier of the TP is built according to table 2.

**Table 2: TP naming convention**

Identifier	TP_<root>_<tgt>_<gr>_<sgr>_<rn>_<sn>_<x>[_<v>]		
	<root> = root	SEC	
	<tgt> = target	ITSS	ITS-S data transfer
		CA	Certificate Authority tests
		AA	ITS-S - AA authorization
		EA	ITS-S - EA enrolment
	<gr> = group	SND	Sending behaviour
		RCV	Receiving behaviour
	<sgr> =sub- group	MSG	Generic messages
		CAM	CAM testing
		DENM	DENM testing
		CERT	Certificate testing
	<sn> = test purpose sequential number		01 to 99
	<x> = category	BV	Valid Behaviour tests
		BO	Invalid Behaviour Tests
	<v> = variant (optional)		A to Z



### 5.1.3 Rules for the behaviour description

The description of the TP is built according to ETSI EG 202 798 [i.1].

ETSI TS 103 097 [1] does not use the finite state machine concept. As a consequence, the test purposes use a generic "Initial State" that corresponds to a state where the IUT is ready for starting the test execution. Furthermore, the IUT shall be left in this "Initial State", when the test is completed.

Being in the "Initial State" refers to the starting point of the initial device configuration. There are no pending actions, no instantiated buffers or variables, which could disturb the execution of a test.

### 5.1.4 Sources of TP definitions

All TPs have been specified according to ETSI TS 103 097 [1] and IEEE Std 1609.2 [2].

### 5.1.5 Mnemonics for PICS reference

To avoid an update of all TPs when the PICS document is changed, table 3 introduces mnemonics name and the correspondence with the real PICS item number. The 'PICS item' as defined in IEEE Std 1609.2 [2], ETSI TS 103 096-1 [3] and ETSI TS 102 871-1 [4] shall be used to determine the test applicability.

**Table 3: Mnemonics for PICS reference**

	<b>Mnemonic</b>	<b>PICS item</b>
1	PICS_GN_SECURITY	A.2/1 [4]
2	PICS_SEC_CERTIFICATE_SELECTION	A.8/1 [3]
3	PICS_SEC_CIRCULAR_REGION	S1.2.2.5.1.1 [2]
4	PICS_SEC_RECTANGULAR_REGION	S1.2.2.5.1.2 [2]
5	PICS_SEC_POLYGONAL_REGION	S1.2.2.5.1.3 [2]
6	PICS_SEC_IDENTIFIED_REGION	S1.2.2.5.1.4 [2]
7	PICS_SEC_ITS_AID_OTHER	A.7/1 [3]
8	PICS_SEC_SHA256	S1.2.2.1.1 [2]
9	PICS_SEC_SHA384	S1.2.2.1.2 [2]
10	PICS_SEC_BRAINPOOL_P256R1	S1.2.2.4.1.2 [2]
11	PICS_SEC_BRAINPOOL_P384R1	S1.2.2.4.2 [2]
12	PICS_SEC_IMPLICIT_CERTIFICATE	S1.2.2.8 [2]

## 6 ITS-S Security

### 6.1 Overview

#### 6.1.1 Certificates content

##### 6.1.1.1 Root Certificate Authorities certificates

RCA certificate	Content	To be installed on the IUT
<b>CERT_IUT_A_RCA</b>	<ul style="list-style-type: none"> <li>- self-signed</li> <li>- name "ETSI Test RCA A certificate"</li> <li>- application permissions:               <ul style="list-style-type: none"> <li>o CRL with SSP 0x01</li> <li>o CTL with SSP 0x0138</li> </ul> </li> <li>- certificate issuing permissions:               <ul style="list-style-type: none"> <li>o CAM with all possible SPP (0x01FFFC / 0xFF0003)</li> <li>o DENM with all possible SSP (0x01FFFFFF / 0xFF000000)</li> <li>o SPATEM with all possible SSP (0x01E0 / 0xFF1F)</li> <li>o MAPEM with all possible SSP (0x01C0 / 0xFF3F)</li> <li>o IVIM with all possible SSP (0x01000000FFF8 / 0xFF000000007)</li> <li>o SREM with all possible SSP (0x01FFFFE0 / 0xFF00001F)</li> <li>o SSEM with all possible SSP (0x01 / 0xFF)</li> <li>o GPC with all possible SSP (0x01 / 0xFF)</li> <li>o GN-MGMT without SSP</li> <li>o CRT-REQ with SSP (0x01FE / 0xFF01)</li> </ul> </li> <li>- validation time for 3 years</li> <li>- no region restriction</li> <li>- assurance level 6</li> <li>- verification key of type compressed with NIST P256R curve</li> <li>- valid signature of type x-only with NIST P256R curve</li> </ul>	Yes
<b>CERT_IUT_A_RCA_A8</b>	Same as CERT_IUT_A_ATCERT_IUT_A_RCA, excepting the following: <ul style="list-style-type: none"> <li>o certificate issuing permissions:               <ul style="list-style-type: none"> <li>o same as in CERT_IUT_A_RCA</li> <li>o unallocated ITS AIDs: 96, 97, 98, 99, 100, 101, 102 without SSP</li> </ul> </li> </ul>	Yes
<b>CERT_IUT_C_RCA</b>	Same as CERT_IUT_A_ATCERT_IUT_A_RCA, excepting the following: <ul style="list-style-type: none"> <li>- rectangular region restriction (10 km square)</li> <li>- no unallocated ITS AID in certificate issuing permissions</li> </ul>	Yes

## 6.1.1.2 Authorization Authorities certificates

AA certificate	Content	To be installed on the IUT
<b>CERT_IUT_A_AA</b>	<ul style="list-style-type: none"> <li>- signer digest of the CERT_IUT_A_RCA</li> <li>- application permissions:               <ul style="list-style-type: none"> <li>o CRT_REQ with SSP 0x0132</li> </ul> </li> <li>- certificate issuing permissions:               <ul style="list-style-type: none"> <li>o CAM with all possible SPP (0x01FFFC / 0xFF0003)</li> <li>o DENM with all possible SSP (0x01FFFFFF / 0xFF000000)</li> <li>o SPATEM with all possible SSP (0x01E0 / 0xFF1F)</li> <li>o MAPEM with all possible SSP (0x01C0 / 0xFF3F)</li> <li>o IVIM with all possible SSP (0x01000000FFF8 / 0xFF000000007)</li> <li>o SREM with all possible SSP (0x01FFFFE0 / 0xFF00001F)</li> <li>o SSEM with all possible SSP (0x01 / 0xFF)</li> <li>o GPC with all possible SSP (0x01 / 0xFF)</li> <li>o GN-MGMT without SSP</li> </ul> </li> <li>- validation time for 3 years</li> <li>- no region restriction</li> <li>- assurance level 4</li> <li>- verification key of type compressed with NIST P256R curve</li> <li>- encryption key of type compressed with NIST P256R curve</li> <li>- valid signature of type x-only with NIST P256R curve</li> </ul>	Yes
<b>CERT_IUT_A_N_AA</b>	Same as CERT_IUT_A_ATCERT_IUT_A_AA, excepting the following: - verification key of type uncompressed	Yes
<b>CERT_IUT_A_B_AA</b>	Same as CERT_IUT_A_ATCERT_IUT_A_AA, excepting the following: - verification key with Brainpool P256r1 curve	Yes
<b>CERT_IUT_A_B3_AA</b>	Same as CERT_IUT_A_ATCERT_IUT_A_B_AA, excepting the following: - verification key with Brainpool P384r1 curve	Yes
<b>CERT_IUT_A_AA_A8</b>	Same as CERT_IUT_A_ATCERT_IUT_A_AA, excepting the following: - signer digest of the CERT_IUT_A_RCA_A8 - certificate issuing permissions: <ul style="list-style-type: none"> <li>o CAM with all possible SPP (0x01FFFC / 0xFF0003)</li> <li>o unallocated ITS AIDs: 96, 97, 98, 99, 100, 101, 102 without SSP</li> <li>o no other certificate issuing permissions</li> </ul>	Yes
<b>CERT_IUT_CC_AA</b>	Same as CERT_IUT_A_ATCERT_IUT_A_AA, excepting the following: - signer digest of the CERT_IUT_C_RCA - rectangular region restriction equal to the one in the CERT_IUT_C_RCA	Yes
<b>CERT_IUT_C3_AA</b>	Same as CERT_IUT_A_ATCERT_IUT_CC_AA, excepting the following: - rectangular region restriction oversizing the one in the CERT_IUT_C_RCA	Yes
<b>CERT_IUT_CA_AA</b>	Same as CERT_IUT_A_ATCERT_IUT_CC_AA, excepting the following: - no region restriction	Yes
<b>CERT_IUT_D_AA</b>	Same as CERT_IUT_A_ATCERT_IUT_CC_AA, excepting the following: - polygonal region restriction as a square with the side of 10 km and center in the IUT position	Yes
<b>CERT_TS_A_AA</b>	Same as CERT_IUT_A_ATCERT_IUT_A_AA. To be used on the Test System side.	Yes
<b>CERT_TS_B_AA</b>	Same as CERT_IUT_A_ATCERT_IUT_A_B_AA. To be used on the Test System side.	Yes
<b>CERT_TS_A_B_AA</b>	Same as CERT_IUT_A_ATCERT_IUT_A_B_AA. To be used on the Test System side.	Yes

## 6.1.1.3 Authorization Tickets

Authorization ticket	Content	To be installed on the IUT
<b>CERT_IUT_A_AT</b>	<ul style="list-style-type: none"> <li>- signer digest of the CERT_IUT_A_AA;</li> <li>- application permissions: <ul style="list-style-type: none"> <li>o CAM with all SPP (0x01FFFC);</li> <li>o DENM with all SSP (0x01FFFFFF);</li> <li>o GN-MGMT;</li> </ul> </li> <li>- validation time for 1 year;</li> <li>- no region restriction;</li> <li>- assurance level 3;</li> <li>- verification key of type compressed with NIST P256R curve ;</li> <li>- encryption key of type compressed with NIST P256R curve;</li> <li>- valid signature of type x-only with NIST P256R curve.</li> </ul>	Yes
<b>CERT_IUT_A_N_AT</b>	Same as CERT_IUT_A_AT CERT_IUT_A_AT, excepting the following: <ul style="list-style-type: none"> <li>- verification key of type uncompressed.</li> </ul>	Yes
<b>CERT_IUT_A_B_AT</b>	Same as CERT_IUT_A_AT CERT_IUT_A_AT, excepting the following: <ul style="list-style-type: none"> <li>- signer digest of the CERT_IUT_A_B_AA;</li> <li>- verification key with Brainpool P256r1 curve;</li> <li>- valid signature with Brainpool P256r1 curve.</li> </ul>	Yes
<b>CERT_IUT_A_B_N_AT</b>	Same as CERT_IUT_A_AT CERT_IUT_A_B_AT, excepting the following: <ul style="list-style-type: none"> <li>- verification key of type uncompressed.</li> </ul>	Yes
<b>CERT_IUT_A_B3_AT</b>	Same as CERT_IUT_A_AT CERT_IUT_A_B_AT, excepting the following: <ul style="list-style-type: none"> <li>- verification key with Brainpool P384r1 curve.</li> </ul>	Yes
<b>CERT_IUT_A_B3_N_AT</b>	Same as CERT_IUT_A_AT CERT_IUT_A_B3_AT, excepting the following: <ul style="list-style-type: none"> <li>- verification key of type uncompressed.</li> </ul>	Yes
<b>CERT_IUT_A_B33_AT</b>	Same as CERT_IUT_A_AT CERT_IUT_A_B3_AT, excepting the following: <ul style="list-style-type: none"> <li>- signer digest of the CERT_IUT_A_B3_AA;</li> <li>- valid signature with Brainpool P384r1 curve.</li> </ul>	Yes
<b>CERT_IUT_A_AT_A8</b>	Same as CERT_IUT_A_AT CERT_IUT_A_AT, excepting the following: <ul style="list-style-type: none"> <li>- signer digest of the CERT_IUT_A_AA_A8;</li> <li>- application permissions: <ul style="list-style-type: none"> <li>o CAM with all SPP (0x01FFFC);</li> <li>o unallocated ITS AIDs: 96, 97, 98, 99, 100, 101, 102 without SSP.</li> </ul> </li> </ul>	Yes
<b>CERT_IUT_B_AT</b>	Same as CERT_IUT_A_AT CERT_IUT_A_AT, excepting the following: <ul style="list-style-type: none"> <li>- circular region restriction with the radius of 5 km and center at the IUT point.</li> </ul>	Yes
<b>CERT_IUT_C_AT</b>	Same as CERT_IUT_A_AT CERT_IUT_A_AT, excepting the following: <ul style="list-style-type: none"> <li>- rectangular region restriction with the side of 5 km and center at the IUT point.</li> </ul>	Yes
<b>CERT_IUT_D_AT</b>	Same as CERT_IUT_A_AT CERT_IUT_A_AT, excepting the following: <ul style="list-style-type: none"> <li>- signer digest of the CERT_IUT_D_AA;</li> <li>- polygonal region restriction identical to the one in the CERT_IUT_D_AA, including the IUT position.</li> </ul>	Yes
<b>CERT_IUT_D_AT_8</b>	Same as CERT_IUT_A_AT CERT_IUT_A_AT, excepting the following: <ul style="list-style-type: none"> <li>- polygonal region restriction contains 8 points.</li> </ul>	Yes
<b>CERT_IUT_E_AT</b>	Same as CERT_IUT_A_AT CERT_IUT_A_AT, excepting the following: <ul style="list-style-type: none"> <li>- identified region restriction including the IUT point.</li> </ul>	Yes
<b>CERT_IUT_E_AT_8</b>	Same as CERT_IUT_A_AT CERT_IUT_E_AT, excepting the following: <ul style="list-style-type: none"> <li>- identified region restriction contains 8 region identifiers.</li> </ul>	Yes
<b>CERT_IUT_A1_AT</b>	Same as CERT_IUT_A_AT CERT_IUT_A_AT, excepting the following: <ul style="list-style-type: none"> <li>- the certificate is expired.</li> </ul>	Yes
<b>CERT_IUT_A2_AT</b>	Same as CERT_IUT_A_AT CERT_IUT_A_AT, excepting the following: <ul style="list-style-type: none"> <li>- the certificate is not valid yet.</li> </ul>	Yes
<b>CERT_IUT_A3_AT</b>	Same as CERT_IUT_A_AT CERT_IUT_A_AT, excepting the following: <ul style="list-style-type: none"> <li>- application permissions: <ul style="list-style-type: none"> <li>o DENM with all SSP (0x01FFFFFF);</li> <li>o GN-MGMT.</li> </ul> </li> </ul>	Yes
<b>CERT_IUT_A4_AT</b>	Same as CERT_IUT_A_AT CERT_IUT_A_AT, excepting the following: <ul style="list-style-type: none"> <li>- application permissions: <ul style="list-style-type: none"> <li>o CAM with all SPP (0x01FFFC);</li> <li>o GN-MGMT.</li> </ul> </li> </ul>	Yes
<b>CERT_IUT_C1_AT</b>	Same as CERT_IUT_A_AT CERT_IUT_A_AT, excepting the following: <ul style="list-style-type: none"> <li>- signer digest of the CERT_IUT_CC_AA;</li> <li>- rectangular region restriction outside of the IUT point.</li> </ul>	Yes

Authorization ticket	Content	To be installed on the IUT
<b>CERT_IUT_C_AT_8</b>	Same as CERT_IUT_A_AT CERT_IUT_A_AT, excepting the following: - rectangular region restriction contains 8 elements.	Yes
<b>CERT_TS_A_AT</b>	Same as CERT_IUT_A_AT CERT_IUT_A_AT To be used on the Test System side.	Yes
<b>CERT_TS_A_B_AT</b>	Same as CERT_IUT_A_AT CERT_TS_A_AT, excepting the following: - verification key with Brainpool P256r1 curve.	Yes
<b>CERT_TS_A_B3_AT</b>	Same as CERT_IUT_A_AT CERT_TS_A_AT, excepting the following: - verification key with Brainpool P384r1 curve.	Yes
<b>CERT_TS_B_AT</b>	Same as CERT_IUT_A_AT CERT_TS_A_AT, excepting the following: - circular region restriction with a radius of 5 km from the IUT point. To be used on the Test System side.	Yes
<b>CERT_TS_B1_AT</b>	Same as CERT_IUT_A_AT CERT_IUT_A_B_AT, excepting the following: - circular region restriction with a radius of 5 km from the base point. To be used on the Test System side.	Yes
<b>CERT_TS_C_AT</b>	Same as CERT_IUT_A_AT CERT_TS_A_AT, excepting the following: - rectangular region restriction with the side of 5 km and center at the IUT point. To be used on the Test System side.	Yes
<b>CERT_TS_D_AT</b>	Same as CERT_IUT_A_AT CERT_TS_A_AT, excepting the following: - polygonal region restriction including the IUT position.	Yes
<b>CERT_TS_E_AT</b>	Same as CERT_IUT_A_AT CERT_TS_A_AT, excepting the following: - identified region restriction including the IUT point.	Yes
<b>CERT_TS_F_AT</b>	Same as CERT_IUT_A_AT CERT_TS_A_AT To be used on the Test System side.	No
<b>CERT_TS_F3_AT</b>	Same as CERT_TS_F_AT, excepting the following: - verification key with Brainpool P384r1 curve. To be used on the Test System side.	No

## 6.2 Sending behaviour

### 6.2.1 General sending behaviour

#### 6.2.1.1 Check the message protocol version

<b>TP Id</b>	TP_SEC_ITSS_SND_MSG_01_BV
<b>Summary</b>	Check that the IUT sends a secured message containing protocol version set to 3
<b>Reference</b>	ETSI TS 103 097 [1], clause 5.1 IEEE Std 1609.2 [2], clause 6.3.2
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>with  the IUT being in the 'authorized' state  ensure that  when  the IUT is requested to send a secured message  then  the IUT sends a EtsiTs103097Data  containing protocolVersion  indicating value '3'</p>	

## 6.2.2 CAM profile

### 6.2.2.1 Check that secured CAM is signed

<b>TP Id</b>	TP_SEC_ITSS_SND_CAM_01_BV
<b>Summary</b>	Check that IUT sends the secured CAM using SignedData container
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.1
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>with  the IUT is authorized with AT certificate (CERT_IUT_A_AT)  ensure that  when  the IUT is requested to send a secured CAM  then  the IUT sends a message of type EtsiTs103097Data  containing content  containing signedData</p>	

### 6.2.2.2 Check secured CAM AID value

<b>TP Id</b>	TP_SEC_ITSS_SND_CAM_02_BV
<b>Summary</b>	Check that IUT sends the secured CAM containing the HeaderInfo field psid set to 'AID_CAM'
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.1
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>with  the IUT is authorized with AT certificate (CERT_IUT_A_AT)  ensure that  when  the IUT is requested to send a secured CAM  then  the IUT sends a message of type EtsiTs103097Data  containing content  containing signedData  containing tbsData  containing headerInfo  containing psid  indicating 'AID_CAM'</p>	

## 6.2.2.3 Check header fields

<b>TP Id</b>	TP_SEC_ITSS_SND_CAM_03_BV
<b>Summary</b>	Check that IUT sends the secured CAM with the HeaderInfo containing generationTime and does not contain expiryTime, generationLocation, encryptionKey, p2pcdLearningRequest, missingCrIIdentifier
<b>Reference</b>	ETSI TS 103 097 [1], clauses 5.2 and 7.1.1
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>with  the IUT is authorized with AT certificate (CERT_IUT_A_AT)  ensure that  when  the IUT is requested to send a secured CAM  then  the IUT sends a message of type EtsiTs103097Data  containing content  containing signedData  containing tbsData  containing headerInfo  containing generationTime  and not containing expiryTime  and not containing generationLocation,  and not containing encryptionKey  and not containing p2pcdLearningRequest  and not containing missingCrIIdentifier</p>	

## 6.2.2.4 Check signer information

<b>TP Id</b>	TP_SEC_ITSS_SND_CAM_04_BV
<b>Summary</b>	Check that IUT sends the secured CAM containing signer containing either certificate or digest Check that signing certificate has permissions to sign CAM messages
<b>Reference</b>	ETSI TS 103 097 [1], clauses 5.2 and 7.1.1 IEEE Std 1609.2 [2], clause 6.3.4
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>with  the IUT is authorized with AT certificate (CERT_IUT_A_AT)  ensure that  when  the IUT is requested to send a secured CAM  then  the IUT sends a message of type EtsiTs103097Data  containing content  containing signedData  containing signer  containing digest  or containing certificate  containing id  indicating 'none'  containing toBeSigned  containing appPermissions  containing the item of type PsidSsp  containing psid  indicating AID_CAM  and not containing certIssuePermissions</p>	

<b>TP Id</b>	TP_SEC_ITSS_SND_CAM_05_BV			
<b>Summary</b>	Check that IUT calculates the digest of certificate using proper hash algorithm Check that IUT canonicalizes certificates before hash calculation			
<b>Reference</b>	ETSI TS 103 097 [1], clauses 5.2 and 7.1.1 IEEE Std 1609.2 [2], clause 6.3.4			
<b>PICS Selection</b>	PICS_GN_SECURITY AND <b>X_PICS</b>			
<b>Expected behaviour</b>				
<p>with</p> <ul style="list-style-type: none"> <li>the IUT is authorized with AT certificate (<b>X_CERTIFICATE</b>)</li> <li>and the IUT is configured to send more than one CAM per second</li> <li>and the IUT having sent a secured CAM <ul style="list-style-type: none"> <li>containing signer <ul style="list-style-type: none"> <li>containing certificate <ul style="list-style-type: none"> <li>indicating <b>X_CERTIFICATE</b></li> <li>containing verifyKeyIndicator <ul style="list-style-type: none"> <li>containing verificationKey <ul style="list-style-type: none"> <li>containing <b>X_KEY</b></li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> <p>ensure that</p> <ul style="list-style-type: none"> <li>when <ul style="list-style-type: none"> <li>the IUT is requested to send a subsequent secured CAM <ul style="list-style-type: none"> <li>containing signer <ul style="list-style-type: none"> <li>containing digest</li> </ul> </li> </ul> </li> </ul> </li> <li>then <ul style="list-style-type: none"> <li>the IUT sends a message of type EtsiTs103097Data <ul style="list-style-type: none"> <li>containing content <ul style="list-style-type: none"> <li>containing signedData <ul style="list-style-type: none"> <li>containing signer <ul style="list-style-type: none"> <li>containing digest <ul style="list-style-type: none"> <li>indicating last 8 bytes of the Hash value calculated using <b>X_HASH</b> algorithm</li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul>				
<b>Permutation table</b>				
<b>XX</b>	<b>X_CERTIFICATE</b>	<b>X_KEY</b>	<b>X_HASH</b>	<b>X_PICS</b>
A	CERT_IUT_A_AT	ecdsaNistP256	SHA-256	
AN	CERT_IUT_A_N_AT	ecdsaNistP256 (uncompressed)	SHA-256	
B	CERT_IUT_A_B_AT	ecdsaBrainpoolP256r1	SHA-256	PICS_SEC_BRAINPOOL_P256R1
BN	CERT_IUT_A_B_N_AT	ecdsaBrainpoolP256r1 (uncompressed)	SHA-256	PICS_SEC_BRAINPOOL_P256R1
C	CERT_IUT_A_B3_AT	ecdsaBrainpoolP384r1	SHA-384	PICS_SEC_SHA384 AND PICS_SEC_BRAINPOOL_P384R1
CN	CERT_IUT_A_B3_N_AT	ecdsaBrainpoolP384r1 (uncompressed)	SHA-384	PICS_SEC_SHA384 AND PICS_SEC_BRAINPOOL_P384R1

<b>TP Id</b>	TP_SEC_ITSS_SND_CAM_06_BV			
<b>Summary</b>	Check that IUT sends the secured CAM containing the signing certificate when over the time of one second no other secured CAM contained the certificate was sent			
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.1			
<b>PICS Selection</b>	PICS_GN_SECURITY			
<b>Expected behaviour</b>				
<p>with</p> <ul style="list-style-type: none"> <li>the IUT is authorized with AT certificate (CERT_IUT_A_AT)</li> <li>and the IUT is configured to send more than one CAM per second</li> <li>and the IUT having sent a secured CAM <ul style="list-style-type: none"> <li>containing generationTime <ul style="list-style-type: none"> <li>indicating TIME_LAST</li> </ul> </li> </ul> </li> </ul> <p>ensure that</p> <ul style="list-style-type: none"> <li>when <ul style="list-style-type: none"> <li>the IUT is sending secured CAM as a message of type EtsiTs103097Data <ul style="list-style-type: none"> <li>containing signer <ul style="list-style-type: none"> <li>containing certificate</li> </ul> </li> </ul> </li> </ul> </li> <li>then <ul style="list-style-type: none"> <li>this message is <ul style="list-style-type: none"> <li>containing headerInfo <ul style="list-style-type: none"> <li>containing generationTime <ul style="list-style-type: none"> <li>indicating TIME (TIME &gt;= TIME_LAST + 1 sec)</li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul>				



<b>TP Id</b>	TP_SEC_ITSS_SND_CAM_07_BV
<b>Summary</b>	Check that IUT sends the secured CAM containing the signing certificate when the timeout of one second has been expired after the previous CAM containing the certificate
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.1
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>with</p> <ul style="list-style-type: none"> <li>the IUT is authorized with AT certificate (CERT_IUT_A_AT)</li> <li>and the IUT is configured to send more than one CAM per second</li> <li>and the IUT having sent a secured CAM <ul style="list-style-type: none"> <li>containing signer</li> <li>containing certificate</li> <li>and containing generationTime</li> <li>indicating TIME_LAST</li> </ul> </li> </ul> <p>ensure that</p> <ul style="list-style-type: none"> <li>when <ul style="list-style-type: none"> <li>the IUT is sending a secured CAM as a message of type EtsiTs103097Data <ul style="list-style-type: none"> <li>containing generationTime</li> <li>indicating TIME &gt;= TIME_LAST + 1 sec</li> </ul> </li> </ul> </li> <li>then <ul style="list-style-type: none"> <li>this message is <ul style="list-style-type: none"> <li>containing certificate</li> </ul> </li> </ul> </li> </ul>	

#### 6.2.2.5 Check that IUT sends certificate to unknown ITS-S

<b>TP Id</b>	TP_SEC_ITSS_SND_CAM_08_BV
<b>Summary</b>	Check that IUT sends the secured CAM containing the signing certificate when the IUT received a CAM from an unknown ITS-S
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.1
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>with</p> <ul style="list-style-type: none"> <li>the IUT is authorized with AT certificate (CERT_IUT_A_AT)</li> <li>and the IUT is configured to send more than one CAM per second</li> <li>and the IUT having already sent secured CAM <ul style="list-style-type: none"> <li>containing certificate</li> <li>at TIME_1</li> </ul> </li> <li>and the IUT having received a message of type EtsiTs103097Data <ul style="list-style-type: none"> <li>containing signedData <ul style="list-style-type: none"> <li>containing signer</li> <li>containing digest</li> <li>indicating HashedId8 value</li> <li>referencing an unknown certificate (CERT_TS_F_AT)</li> <li>at TIME_2 (TIME_1 &lt; TIME_2 &lt; TIME_1+1 sec)</li> </ul> </li> </ul> </li> </ul> <p>ensure that</p> <ul style="list-style-type: none"> <li>when <ul style="list-style-type: none"> <li>the IUT is requested to send secured CAM <ul style="list-style-type: none"> <li>at TIME_3 (TIME_1 &lt; TIME_2 &lt; TIME_3 &lt; TIME_1 + 1 sec)</li> </ul> </li> </ul> </li> <li>then <ul style="list-style-type: none"> <li>the IUT sends a message of type EtsiTs103097Data <ul style="list-style-type: none"> <li>containing signedData</li> <li>containing signer</li> <li>containing certificate</li> </ul> </li> </ul> </li> </ul>	

## 6.2.2.6 Check that IUT restarts the timer when the certificate has been sent

<b>TP Id</b>	TP_SEC_ITSS_SND_CAM_09_BV
<b>Summary</b>	Check that IUT restarts the certificate sending timer when the signing certificate was sent
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.1
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>with</p> <ul style="list-style-type: none"> <li>the IUT is authorized with AT certificate (CERT_IUT_A_AT)</li> <li>and the IUT is configured to send more than one CAM per second</li> <li>and the IUT having already sent secured CAM <ul style="list-style-type: none"> <li>containing signer</li> <li>containing certificate</li> </ul> </li> <li>at TIME_1</li> <li>and the IUT having received a secured CAM <ul style="list-style-type: none"> <li>containing signer</li> <li>containing digest</li> <li>indicating HashID8 value</li> <li>referencing an unknown certificate (CERT_TS_F_AT)</li> </ul> </li> <li>at TIME_2 (TIME_1 + 0,3 sec of tolerance)</li> <li>and the IUT having sent secured CAM <ul style="list-style-type: none"> <li>containing signer</li> <li>containing certificate</li> </ul> </li> <li>at TIME_3 (TIME_3 &gt; TIME_2)</li> </ul> <p>ensure that</p> <ul style="list-style-type: none"> <li>when <ul style="list-style-type: none"> <li>the IUT is sending the next secured CAM <ul style="list-style-type: none"> <li>containing signedData</li> <li>containing signer</li> <li>containing certificate</li> </ul> </li> <li>at TIME_4</li> </ul> </li> <li>then <ul style="list-style-type: none"> <li>the difference between TIME_4 and TIME_3 is about 1 sec</li> </ul> </li> </ul>	

## 6.2.2.7 Check sending certificate request for unknown certificate

<b>TP Id</b>	TP_SEC_ITSS_SND_CAM_10_BV
<b>Summary</b>	Check that the IUT sends certificate request when it receives secured CAM containing digest of unknown certificate as a message signer
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.1 IEEE Std 1609.2 [2], clauses 6.3.9 and 8.2.4.1.2
<b>PICS Selection</b>	PICS_GN_SECURITY, PICS_SEC_P2P_AT_DISTRIBUTION
<b>Expected behaviour</b>	
<p>with</p> <ul style="list-style-type: none"> <li>the IUT is authorized with AT certificate (CERT_IUT_A_AT)</li> <li>and the IUT has receiving a EtsiTs103097Data <ul style="list-style-type: none"> <li>containing signer</li> <li>containing digest</li> <li>indicating HashedId8 value <b>DIGEST_F</b></li> <li>referencing an unknown certificate (CERT_TS_F_AT)</li> </ul> </li> </ul> <p>ensure that</p> <ul style="list-style-type: none"> <li>when <ul style="list-style-type: none"> <li>the IUT is requested to send a secured CAM</li> </ul> </li> <li>then <ul style="list-style-type: none"> <li>the IUT sends a message of type EtsiTs103097Data <ul style="list-style-type: none"> <li>containing headerInfo</li> <li>containing inlineP2pcdRequest</li> <li>containing HashedId3 value</li> <li>indicating last 3 octets of <b>DIGEST_F</b></li> </ul> </li> </ul> </li> </ul>	

<b>TP Id</b>	TP_SEC_ITSS_SND_CAM_11_BV_XX		
<b>Summary</b>	Check that the IUT sends certificate request when it receives secured CAM containing certificate signed by unknown AA certificate		
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.1 IEEE Std 1609.2 [2], clauses 6.3.9 and 8.2.4.1.2		
<b>PICS Selection</b>	PICS_GN_SECURITY AND PICS_SEC_P2P_AA_DISTRIBUTION AND <b>X_PICS</b>		
<b>Expected behaviour</b>			
<p>with</p> <ul style="list-style-type: none"> <li>the IUT is authorized with AT certificate (CERT_IUT_A_AT)</li> <li>and the IUT has receiving a message of type EtsiTs103097Data <ul style="list-style-type: none"> <li>containing signer <ul style="list-style-type: none"> <li>containing certificate <ul style="list-style-type: none"> <li>containing issuer <ul style="list-style-type: none"> <li>containing <b>X_FIELD_1</b> <ul style="list-style-type: none"> <li>indicating HashedId8 value <b>DIGEST_F</b> <ul style="list-style-type: none"> <li>referencing an unknown certificate (<b>X_CERT</b>CERT_TS_F_AT)</li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> <p>ensure that</p> <ul style="list-style-type: none"> <li>when <ul style="list-style-type: none"> <li>the IUT is requested to send secured CAM</li> </ul> </li> <li>then <ul style="list-style-type: none"> <li>the IUT sends a message of type EtsiTs103097Data <ul style="list-style-type: none"> <li>containing signedData <ul style="list-style-type: none"> <li>containing tbsData <ul style="list-style-type: none"> <li>containing headerInfo <ul style="list-style-type: none"> <li>containing inlineP2pcdRequest <ul style="list-style-type: none"> <li>containing HashedId3 value <ul style="list-style-type: none"> <li>indicating last 3 octets of <b>DIGEST_F</b></li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul>			
<b>Permutation table</b>			
<b>XX</b>	<b>X_FIELD_1</b>	<b>X_CERT</b>	<b>X_PICS</b>
A	sha256AndDigest	CERT_TS_F_AT	
B	sha384AndDigest	CERT_TS_F3_AT	PICS_SEC_SHA384

## 6.2.2.8 Check that IUT sends AT certificate when requested

<b>TP Id</b>	TP_SEC_ITSS_SND_CAM_12_BV
<b>Summary</b>	Check that IUT sends the secured CAM containing the signing certificate when it received a CAM containing a request for unrecognized certificate that matches with the currently used AT certificate ID of the IUT
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.1 IEEE Std 1609.2 [2], clauses 6.3.9 and 8.2.4.2.3
<b>PICS Selection</b>	PICS_GN_SECURITY AND PICS_SEC_P2P_AT_DISTRIBUTION
<b>Expected behaviour</b>	
<p>with</p> <ul style="list-style-type: none"> <li>the IUT is authorized with AT certificate (CERT_IUT_A_AT)</li> <li>and the IUT is configured to send more than one CAM per second</li> <li>and the IUT having already sent secured CAM <ul style="list-style-type: none"> <li>containing signer</li> <li>containing certificate</li> </ul> </li> <li>at TIME_1</li> <li>and the IUT having received a secured CAM <ul style="list-style-type: none"> <li>containing headerInfo <ul style="list-style-type: none"> <li>containing inlineP2pcdRequest <ul style="list-style-type: none"> <li>containing HashedId3 <ul style="list-style-type: none"> <li>indicating last 3 octets of currently used AT certificate (<b>HASHED_ID_3</b>)</li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> <li>at TIME_2 (TIME_1 &lt; TIME_2 &lt; TIME_1+1 sec)</li> </ul> <p>ensure that</p> <ul style="list-style-type: none"> <li>when <ul style="list-style-type: none"> <li>the IUT is requested to send a CAM <ul style="list-style-type: none"> <li>at TIME_3 (TIME_1 &lt; TIME_2 &lt; TIME_3 &lt; TIME_1+1 sec)</li> </ul> </li> </ul> </li> <li>then <ul style="list-style-type: none"> <li>the IUT sends a SecuredMessage of type EtsiTs103097Data <ul style="list-style-type: none"> <li>containing signer</li> <li>and containing certificate <ul style="list-style-type: none"> <li>referenced by the HashedId3 value <b>HASHED_ID_3</b></li> </ul> </li> </ul> </li> </ul> </li> </ul>	

## 6.2.2.9 Check that IUT sends AA certificate when requested

<b>TP Id</b>	TP_SEC_ITSS_SND_CAM_13_BV
<b>Summary</b>	Check that IUT sends the secured CAM containing the AA certificate in the requestedCertificate headerInfo field when it received a CAM containing a request for unrecognized certificate that matches with the currently used AA certificate ID of the IUT
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.1 IEEE Std 1609.2 [2], clauses 6.3.9 and 8.2.4.2.3
<b>PICS Selection</b>	PICS_GN_SECURITY AND PICS_SEC_P2P_AT_DISTRIBUTION
<b>Expected behaviour</b>	
<p>with</p> <ul style="list-style-type: none"> <li>the IUT is authorized with AT certificate (CERT_IUT_A_AT) issued by the AA certificate (CERT_IUT_A_AA)</li> <li>and the IUT is configured to send more than one CAM per second</li> <li>and the IUT having already sent a secured CAM <ul style="list-style-type: none"> <li>containing signer</li> <li>containing certificate</li> <li>at TIME_1</li> </ul> </li> <li>and the IUT having received a secured CAM <ul style="list-style-type: none"> <li>containing headerInfo <ul style="list-style-type: none"> <li>containing inlineP2pcdRequest</li> <li>containing HashedId3 value <ul style="list-style-type: none"> <li>indicating last 3 octets of the digest of CERT_IUT_A_AA</li> </ul> </li> </ul> </li> <li>at TIME_2 (TIME_1 &lt; TIME_2 &lt; TIME_1+1 sec)</li> </ul> </li> </ul> <p>ensure that</p> <ul style="list-style-type: none"> <li>when <ul style="list-style-type: none"> <li>the IUT is requested to send a secured CAM</li> <li>at TIME_3 (TIME_1 &lt; TIME_2 &lt; TIME_3 &lt; TIME_1+1 sec)</li> </ul> </li> <li>then <ul style="list-style-type: none"> <li>the IUT sends a SecuredMessage of type EtsiTs103097Data <ul style="list-style-type: none"> <li>containing headerInfo <ul style="list-style-type: none"> <li>containing requestedCertificate</li> <li>indicating requested AA certificate CERT_IUT_A_AA</li> </ul> </li> </ul> </li> </ul> </li> </ul>	

<b>TP Id</b>	TP_SEC_ITSS_SND_CAM_14_BV
<b>Summary</b>	Check that IUT sends the secured CAM containing the AA certificate in the requestedCertificate headerInfo field when it received a CAM containing a request for unrecognized certificate that matches with the known AA certificate ID which is not currently used by the IUT
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.1 IEEE Std 1609.2 [2], clauses 6.3.9 and 8.2.4.2.3
<b>PICS Selection</b>	PICS_GN_SECURITY AND PICS_SEC_P2P_AA_DISTRIBUTION
<b>Expected behaviour</b>	
<p>with</p> <ul style="list-style-type: none"> <li>the IUT is authorized with AT certificate (CERT_IUT_A_AT)</li> <li>and the IUT is configured to send more than one CAM per second</li> <li>and the IUT is configured to know the AA certificate (CERT_IUT_A_N_AA)</li> <li>and the IUT has already sent secured CAM <ul style="list-style-type: none"> <li>containing signer</li> <li>containing certificate</li> </ul> </li> <li>at TIME_1</li> <li>and the IUT having received a secured CAM <ul style="list-style-type: none"> <li>containing headerInfo <ul style="list-style-type: none"> <li>containing inlineP2pcdRequest <ul style="list-style-type: none"> <li>containing HashedId3 value <ul style="list-style-type: none"> <li>indicating last 3 octets of the digest of CERT_IUT_A_N_AA <ul style="list-style-type: none"> <li>which is not an issuer of currently used AT certificate</li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> <li>at TIME_2 (TIME_1 &lt; TIME_2 &lt; TIME_1+1 sec)</li> </ul> <p>ensure that</p> <ul style="list-style-type: none"> <li>when <ul style="list-style-type: none"> <li>the IUT is requested to send a secured CAM <ul style="list-style-type: none"> <li>at TIME_3 (TIME_1 &lt; TIME_2 &lt; TIME_3 &lt; TIME_1+1 sec)</li> </ul> </li> </ul> </li> <li>then <ul style="list-style-type: none"> <li>the IUT sends a SecuredMessage of type EtsiTs103097Data <ul style="list-style-type: none"> <li>containing headerInfo <ul style="list-style-type: none"> <li>containing requestedCertificate <ul style="list-style-type: none"> <li>indicating requested AA certificate (CERT_IUT_A_N_AA)</li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul>	

<b>TP Id</b>	TP_SEC_ITSS_SND_CAM_15_BV
<b>Summary</b>	Check that the IUT does not send a secured CAM containing the AA certificate in the requestedCertificate headerInfo field when it was previously requested and already received from another ITS-S
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.1 IEEE Std 1609.2 [2], clauses 6.3.9 and 8.2.4.2.3
<b>PICS Selection</b>	PICS_GN_SECURITY, PICS_SEC_P2P_AA_DISTRIBUTION
<b>Expected behaviour</b>	
<p>with</p> <ul style="list-style-type: none"> <li>the IUT is authorized with AT certificate (CERT_IUT_A_AT) issued by the AA certificate (CERT_IUT_A_AA)</li> <li>and the IUT is configured to send more than one CAM per second</li> <li>and the IUT having already sent secured CAM containing signer containing certificate at TIME_1</li> <li>and the IUT having received a secured CAM containing headerInfo containing inlineP2pcdRequest containing HashedId3 value indicating last 3 octets of the digest of CERT_IUT_A_AA at TIME_2 (TIME_1 &lt; TIME_2 &lt; TIME_1 + 0,8 sec)</li> <li>and the IUT having received a secured CAM containing headerInfo containing requestedCertificate indicating requested AA certificate (CERT_IUT_A_AA) at TIME_3 (TIME_2 &lt; TIME_3 &lt; TIME_2 + 0,1 sec)</li> </ul> <p>ensure that</p> <ul style="list-style-type: none"> <li>when the IUT is requested to send a secured CAM at TIME_4 (TIME_3 &lt; TIME_4 &lt; TIME_1 + 0,9 sec)</li> <li>then the IUT sends a SecuredMessage of type EtsiTs103097Data containing headerInfo not containing requestedCertificate</li> </ul>	

<b>TP Id</b>	TP_SEC_ITSS_SND_CAM_16_BV
<b>Summary</b>	Check that the IUT does not send a secured CAM containing the AA certificate in the requestedCertificate headerInfo field when it contains certificate in the signer field
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.1 IEEE Std 1609.2 [2], clauses 6.3.9 and 8.2.4.2.3
<b>PICS Selection</b>	PICS_GN_SECURITY, PICS_SEC_P2P_AA_DISTRIBUTION
<b>Expected behaviour</b>	
<p>with</p> <ul style="list-style-type: none"> <li>the IUT is authorized with AT certificate (CERT_IUT_A_AT) issued by the AA certificate (CERT_IUT_A_AA)</li> <li>and the IUT is configured to send more than one CAM per second</li> <li>and the IUT having already sent a secured CAM containing signer containing certificate at TIME_1</li> <li>and the IUT having received a SecuredMessage containing headerInfo containing inlineP2pcdRequest containing HashedId3 value indicating last 3 octets of the digest of CERT_IUT_A_AA at TIME_2 (TIME2 = TIME_1 + 0,9 sec)</li> </ul> <p>ensure that</p> <ul style="list-style-type: none"> <li>when the IUT is requested to send a secured CAM at TIME_3 (TIME_2 &lt; TIME_3 &lt; TIME_1 + 1 sec)</li> </ul> <p>then</p> <ul style="list-style-type: none"> <li>the IUT sends a SecuredMessage of type EtsiTs103097Data containing signer containing certificate and containing headerInfo <b>not</b> containing requestedCertificate</li> </ul>	

<b>TP Id</b>	TP_SEC_ITSS_SND_CAM_17_BV
<b>Summary</b>	Check that the IUT sends a secured CAM containing the AA certificate in the requestedCertificate headerInfo field with the next CAM containing digest as a signer info
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.1 IEEE Std 1609.2 [2], clauses 6.3.9 and 8.2.4.2.3
<b>PICS Selection</b>	PICS_GN_SECURITY, PICS_SEC_P2P_AA_DISTRIBUTION
<b>Expected behaviour</b>	
<p>with</p> <ul style="list-style-type: none"> <li>the IUT is authorized with AT certificate (CERT_IUT_A_AT) issued by the AA certificate (CERT_IUT_A_AA)</li> <li>and the IUT is configured to send more than one CAM per second</li> <li>and the IUT having already sent secured CAM containing signer containing certificate at TIME_1</li> <li>and the IUT having received a SecuredMessage of type EtsiTs103097Data containing headerInfo containing inlineP2pcdRequest containing HashedId3 value indicating last 3 octets of the digest of CERT_IUT_A_AA at TIME_2 (TIME_1+0,9 sec &lt; TIME2 &lt; TIME_1 + 1 sec)</li> </ul> <p>ensure that</p> <ul style="list-style-type: none"> <li>when the IUT is sending a first subsequent secured CAM containing signer containing digest</li> </ul> <p>then</p> <ul style="list-style-type: none"> <li>this message containing headerInfo containing requestedCertificate indicating requested AA certificate CERT_IUT_A_AA</li> </ul>	



## 6.2.2.10 Check generation time

<b>TP Id</b>	TP_SEC_ITSS_SND_CAM_18_BV
<b>Summary</b>	Check that IUT sends the secured CAM containing generation time and this time is inside the validity period of the signing certificate Check that message generation time value is realistic
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.1 IEEE Std 1609.2 [2], clauses 5.2.3.2.2, 5.2.4.2.2 and 5.2.4.2.3
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>with  the IUT is authorized with AT certificate (CERT_IUT_A_AT)  ensure that  when  the IUT is requested to send CAM  containing certificate  then  the IUT sends a SecuredMessage of type EtsiTs103097Data  containing headerInfo  containing generationTime  indicating GEN_TIME (CUR_TIME - 5 min &lt;= GEN_TIME &lt;= CUR_TIME + 5 min)  and containing signer  containing certificate  containing toBeSigned  containing validityPeriod  containing start  indicating value X_START_VALIDITY (X_START_VALIDITY &lt;= GEN_TIME)  and containing duration  indicating value &gt; GEN_TIME - X_START_VALIDITY</p>	

## 6.2.2.11 Check payload

<b>TP Id</b>	TP_SEC_ITSS_SND_CAM_19_BV
<b>Summary</b>	Check that IUT sends the secured CAM containing the 'data' field in signed data payload, containing the EtsiTs103097Data of type unsecured, contained the CAM payload
<b>Reference</b>	ETSI TS 103 097 [1], clauses 5.2 and 7.1.1
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>with  the IUT is authorized with AT certificate (CERT_IUT_A_AT)  ensure that  when  the IUT is requested to send a secured CAM  then  the IUT sends a message of type EtsiTs103097Data  contains content  contains signedData  containing tbsData  containing payload  containing data  containing content  containing unsecuredData  containing not-empty data</p>	

## 6.2.2.12 Check signing permissions

<b>TP Id</b>	TP_SEC_ITSS_SND_CAM_20_BV
<b>Summary</b>	Check that the IUT sends the secured CAM signed with the certificate containing appPermissions allowing to sign CA messages
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.2.1 IEEE Std 1609.2 [2], clause 5.2.3.2.2
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>with  the IUT is authorized with AT certificate (CERT_IUT_A_AT)  ensure that  when  the IUT is requested to send a secured CAM  then  the IUT sends a message of type EtsiTs103097Data  containing signer  containing certificate  containing appPermissions  containing an item of type PsidSsp  containing psid = AID_CAM</p>	

## 6.2.2.13 Check signature

<b>TP Id</b>	TP_SEC_ITSS_SND_CAM_21_BV_XX			
<b>Summary</b>	Check that IUT sends the secured CAM containing signature Check that the signature is calculated over the right fields and using right hash algorithm by cryptographically verifying the signature			
<b>Reference</b>	ETSI TS 103 097 [1], clauses 5.2, 7.1.1 IEEE Std 1609.2 [2], clauses 5.3.1, 6.3.4, 6.3.29, 6.3.30 and 6.3.31			
<b>PICS Selection</b>	PICS_GN_SECURITY AND <b>X_PICS</b>			
<b>Expected behaviour</b>				
<p>with  the IUT is authorized with AT certificate (<b>X_CERTIFICATE</b>)  containing verifyKeyIndicator  containing verificationKey  containing <b>X_KEY</b>  indicating KEY</p> <p>ensure that  when  the IUT is requested to send a secured CAM  then  the IUT sends a message of type EtsiTs103097Data  containing signedData  containing signer  containing digest  referencing the certificate <b>X_CERTIFICATE</b>  or containing certificate  indicating <b>X_CERTIFICATE</b>  and containing signature  containing <b>X_SIGNATURE</b>  verifiable using KEY</p>				
<b>Permutation table</b>				
<b>XX</b>	<b>X_CERTIFICATE</b>	<b>X_KEY</b>	<b>X_SIGNATURE</b>	<b>X_PICS</b>
A	CERT_IUT_A_AT	ecdsaNistP256	ecdsaNistP256Signature	
B	CERT_IUT_A_B_AT	ecdsaBrainpoolP256r1	ecdsaBrainpoolP256r1Signature	PICS_SEC_BRAINPOOL_P256 R1
C	CERT_IUT_A_B3_AT	ecdsaBrainpoolP384r1	ecdsaBrainpoolP384r1Signature	PICS_SEC_SHA384 AND PICS_SEC_BRAINPOOL_P384 R1

<b>TP Id</b>	TP_SEC_ITSS_SND_CAM_22_BV_XX		
<b>Summary</b>	Check that IUT sends the secured CAM containing signature containing the ECC point of type set to either compressed_lsb_y_0, compressed_lsb_y_1 or x_coordinate_only		
<b>Reference</b>	ETSI TS 103 097 [1], clauses 5.2, 7.1.1 IEEE Std 1609.2 [2], clauses 6.3.30 and 6.3.31		
<b>PICS Selection</b>	PICS_GN_SECURITY AND <b>X_PICS</b>		
<b>Expected behaviour</b>			
<p>with  the IUT is authorized with AT certificate (<b>X_CERTIFICATE</b>)  ensure that  when  the IUT is requested to send a secured CAM  then  the IUT sends a message of type EtsiTs103097Data  containing signedData  containing signature  containing <b>X_SIGNATURE</b>  containing rSig  containing x-only  or containing compressed-y-0  or containing compressed-y-1</p>			
<b>Permutation table</b>			
<b>XX</b>	<b>X_CERTIFICATE</b>	<b>X_SIGNATURE</b>	<b>X_PICS</b>
A	CERT_IUT_A_AT	ecdsaNistP256Signature	
B	CERT_IUT_A_B_AT	ecdsaBrainpoolP256r1Signature	PICS_SEC_BRAINPOOL_P256R1
C	CERT_IUT_A_B3_AT	ecdsaBrainpoolP384r1Signature	PICS_SEC_SHA384 AND PICS_SEC_BRAINPOOL_P384R1

#### 6.2.2.14 Check support for certificate content

<b>TP Id</b>	TP_SEC_ITSS_SND_CAM_23_BV		
<b>Summary</b>	Check that IUT supports at least 8 items in the appPermissions component of the certificate		
<b>Reference</b>	IEEE Std 1609.2 [2], clause 6.4.8		
<b>PICS Selection</b>	PICS_GN_SECURITY		
<b>Expected behaviour</b>			
<p>with  the IUT is authorized with AT certificate (CERT_IUT_A_AT_A8)  containing toBeSigned  containing appPermissions  containing 8 entries  indicating the last item  containing psid  indicating the 'AID_CAM'</p> <p>ensure that  when  the IUT is requested to send a secured CAM  then  the IUT sends a message of type EtsiTs103097Data  containing content  containing signedData  containing tbsData  containing headerInfo  containing psid  indicating 'AID_CAM'</p>			

<b>TP Id</b>	TP_SEC_ITSS_SND_CAM_24_BV
<b>Summary</b>	Check that IUT supports at least 8 items in the certIssuePermissions component of the certificate
<b>Reference</b>	IEEE Std 1609.2 [2], clause 6.4.8
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>with</p> <ul style="list-style-type: none"> <li>the IUT is authorized with AT certificate (CERT_IUT_A_AT_A8) <ul style="list-style-type: none"> <li>containing appPermissions</li> <li>conformed to the certIssuePermissions</li> </ul> </li> <li>issued by AA certificate (CERT_IUT_A_AA_A8) <ul style="list-style-type: none"> <li>containing toBeSigned <ul style="list-style-type: none"> <li>containing certIssuePermissions</li> <li>containing 8 entries <ul style="list-style-type: none"> <li>indicating the last item</li> <li>containing psid</li> <li>indicating the 'AID_CAM'</li> </ul> </li> </ul> </li> </ul> </li> </ul> <p>ensure that</p> <ul style="list-style-type: none"> <li>when <ul style="list-style-type: none"> <li>the IUT is requested to send a secured CAM</li> </ul> </li> <li>then <ul style="list-style-type: none"> <li>the IUT sends a message of type EtsiTs103097Data <ul style="list-style-type: none"> <li>containing content <ul style="list-style-type: none"> <li>containing signedData</li> <li>containing tbsData <ul style="list-style-type: none"> <li>containing headerInfo</li> <li>containing psid</li> <li>indicating 'AID_CAM'</li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul>	

#### 6.2.2.15 Check certificate consistency conditions

<b>TP Id</b>	TP_SEC_ITSS_SND_CAM_23_BV
<b>Summary</b>	Check that IUT does not send secured CAMs if IUT is authorized with AT certificate does not allow sending messages in this location
<b>Reference</b>	IEEE Std 1609.2 [2], clause 5.2.3.2.2
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>with</p> <ul style="list-style-type: none"> <li>the IUT is authorized with AT certificate (CERT_IUT_C1_AT) <ul style="list-style-type: none"> <li>containing region <ul style="list-style-type: none"> <li>indicating rectangular region</li> <li>not containing current IUT position</li> </ul> </li> </ul> </li> <li>and the IUT has no other installed AT certificates</li> </ul> <p>ensure that</p> <ul style="list-style-type: none"> <li>when <ul style="list-style-type: none"> <li>the IUT is requested to send a secured CAM</li> </ul> </li> <li>then <ul style="list-style-type: none"> <li>the IUT does not send CAM</li> </ul> </li> </ul>	

<b>TP Id</b>	TP_SEC_ITSS_SND_CAM_24_BV
<b>Summary</b>	Check that IUT does not send the secured CAM if IUT is configured to use an AT certificate without region validity restriction and generation location is outside of the region of the issuing AA certificate
<b>Reference</b>	IEEE Std 1609.2 [2], clause 5.2.3.2.2
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>with</p> <ul style="list-style-type: none"> <li>the IUT has been authorized with the AT certificate (CERT_IUT_CA3_AT) <ul style="list-style-type: none"> <li>not containing region</li> <li>and issued by the AA certificate (CERT_IUT_C3_AA) <ul style="list-style-type: none"> <li>containing region <ul style="list-style-type: none"> <li>indicating rectangular region</li> <li>not containing current IUT position</li> </ul> </li> </ul> </li> </ul> </li> </ul> <p>ensure that</p> <ul style="list-style-type: none"> <li>when <ul style="list-style-type: none"> <li>the IUT is requested to send a secured CAM</li> </ul> </li> <li>then <ul style="list-style-type: none"> <li>the IUT does not send CAM</li> </ul> </li> </ul>	

<b>TP Id</b>	TP_SEC_ITSS_SND_CAM_25_BV
<b>Summary</b>	Check that IUT does not send secured CAMs if all AT certificates installed on the IUT was expired
<b>Reference</b>	IEEE Std 1609.2 [2], clause 5.2.3.2.2
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>with</p> <ul style="list-style-type: none"> <li>the IUT is authorized with AT certificate (CERT_IUT_A1_AT) <ul style="list-style-type: none"> <li>containing validityPeriod <ul style="list-style-type: none"> <li>indicating start + duration &lt; CURRENT_TIME</li> </ul> </li> <li>and the IUT has no other installed AT certificates</li> </ul> </li> </ul> <p>ensure that</p> <ul style="list-style-type: none"> <li>when <ul style="list-style-type: none"> <li>the IUT is requested to send a secured CAM</li> </ul> </li> <li>then <ul style="list-style-type: none"> <li>the IUT does not send CAM</li> </ul> </li> </ul>	

<b>TP Id</b>	TP_SEC_ITSS_SND_CAM_26_BV
<b>Summary</b>	Check that IUT does not send secured CAMs if all AT certificates installed on the IUT have the starting time in the future
<b>Reference</b>	IEEE Std 1609.2 [2], clause 5.2.3.2.2
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>with</p> <ul style="list-style-type: none"> <li>the IUT is authorized with AT certificate (CERT_IUT_A2_AT) <ul style="list-style-type: none"> <li>containing validityPeriod <ul style="list-style-type: none"> <li>indicating start &gt; CURRENT_TIME</li> </ul> </li> <li>and the IUT has no other installed AT certificates</li> </ul> </li> </ul> <p>ensure that</p> <ul style="list-style-type: none"> <li>when <ul style="list-style-type: none"> <li>the IUT is requested to send a secured CAM</li> </ul> </li> <li>then <ul style="list-style-type: none"> <li>the IUT does not send CAM</li> </ul> </li> </ul>	

<b>TP Id</b>	TP_SEC_ITSS_SND_CAM_27_BV
<b>Summary</b>	Check that IUT does not send secured CAMs if IUT does not possess an AT certificate allowing sending CAM by its appPermissions
<b>Reference</b>	IEEE Std 1609.2 [2], clause 5.2.3.2.2
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>with</p> <ul style="list-style-type: none"> <li>the IUT is authorized with AT certificate (CERT_IUT_A3_AT) <ul style="list-style-type: none"> <li>containing appPermissions</li> <li>not containing PsidSSP</li> <li>containing psid <ul style="list-style-type: none"> <li>indicating AID_CAM</li> </ul> </li> </ul> </li> <li>and the IUT has no other installed AT certificates</li> </ul> <p>ensure that</p> <ul style="list-style-type: none"> <li>when <ul style="list-style-type: none"> <li>the IUT is requested to send a secured CAM</li> </ul> </li> <li>then <ul style="list-style-type: none"> <li>the IUT does not send CAM</li> </ul> </li> </ul>	

## 6.2.3 DENM profile

### 6.2.3.1 Check secured DENM is signed

<b>TP Id</b>	TP_SEC_ITSS_SND_DENM_01_BV
<b>Summary</b>	Check that IUT sends the secured DENM using SignedData container
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.2
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>with</p> <ul style="list-style-type: none"> <li>the IUT is authorized with AT certificate (CERT_IUT_A_AT)</li> </ul> <p>ensure that</p> <ul style="list-style-type: none"> <li>when <ul style="list-style-type: none"> <li>the IUT is requested to send a secured DENM</li> </ul> </li> <li>then <ul style="list-style-type: none"> <li>the IUT sends a EtsiTs103097Data <ul style="list-style-type: none"> <li>containing content</li> <li>containing signedData</li> </ul> </li> </ul> </li> </ul>	

### 6.2.3.2 Check secured DENM AID value

<b>TP Id</b>	TP_SEC_ITSS_SND_DENM_02_BV
<b>Summary</b>	Check that IUT sends the secured DENM containing the HeaderInfo field psid set to 'AID_DENM'
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.2
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>with</p> <ul style="list-style-type: none"> <li>the IUT is authorized with AT certificate (CERT_IUT_A_AT)</li> </ul> <p>ensure that</p> <ul style="list-style-type: none"> <li>when <ul style="list-style-type: none"> <li>the IUT is requested to send a secured DENM</li> </ul> </li> <li>then <ul style="list-style-type: none"> <li>the IUT sends a EtsiTs103097Data <ul style="list-style-type: none"> <li>containing content</li> <li>containing signedData <ul style="list-style-type: none"> <li>containing tbsData <ul style="list-style-type: none"> <li>containing headerInfo <ul style="list-style-type: none"> <li>containing psid <ul style="list-style-type: none"> <li>indicating 'AID_DENM'</li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul>	

## 6.2.3.3 Check header fields

<b>TP Id</b>	TP_SEC_ITSS_SND_DENM_03_BV
<b>Summary</b>	Check that IUT sends the secured DENM with the HeaderInfo containing generationTime and generationLocation and does not contain expiryTime, encryptionKey, p2pcdLearningRequest, missingCrIIdentifier, inlineP2pcdRequest, requestedCertificate
<b>Reference</b>	ETSI TS 103 097 [1], clauses 5.2 and 7.1.2
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>with  the IUT is authorized with AT certificate (CERT_IUT_A_AT)  ensure that  when  the IUT is requested to send a secured DENM  then  the IUT sends a EtsiTs103097Data  containing content  containing signedData  containing tbsData  containing headerInfo  containing generationTime  and containing generationLocation,  and not containing expiryTime  and not containing encryptionKey  and not containing p2pcdLearningRequest  and not containing missingCrIIdentifier  and not containing inlineP2pcdRequest  and not containing requestedCertificate</p>	

## 6.2.3.4 Check signer information

<b>TP Id</b>	TP_SEC_ITSS_SND_DENM_04_BV
<b>Summary</b>	Check that IUT sends the secured DENM containing signer containing certificate
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.2 IEEE Std 1609.2 [2], clause 6.3.4
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>with  the IUT is authorized with AT certificate (CERT_IUT_A_AT)  ensure that  when  the IUT is requested to send a secured DENM  then  the IUT sends a EtsiTs103097Data  containing content  containing signedData  containing signer  containing certificate  containing toBeSigned  containing appPermissions  containing the item of type PsidSsp  containing psid  indicating AID_DENM</p>	

## 6.2.3.5 Check generation time

<b>TP Id</b>	TP_SEC_ITSS_SND_DENM_05_BV
<b>Summary</b>	Check that IUT sends the secured DENM containing generation time and this time is inside the validity period of the signing certificate Check that message generation time value is realistic
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.2 IEEE Std 1609.2 [2], clauses 5.2.3.2.2, 5.2.4.2.2 and 5.2.4.2.3
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>with</p> <ul style="list-style-type: none"> <li>the IUT is authorized with AT certificate (CERT_IUT_A_AT)</li> </ul> <p>ensure that</p> <ul style="list-style-type: none"> <li>when <ul style="list-style-type: none"> <li>the IUT is requested to send a secured DENM</li> </ul> </li> <li>then <ul style="list-style-type: none"> <li>the IUT sends a message of type EtsiTs103097Data <ul style="list-style-type: none"> <li>containing headerInfo <ul style="list-style-type: none"> <li>containing generationTime <ul style="list-style-type: none"> <li>indicating GEN_TIME (<math>CUR\_TIME - 10min \leq GEN\_TIME \leq CUR\_TIME + 10 min</math>)</li> </ul> </li> <li>and containing signer <ul style="list-style-type: none"> <li>containing certificate <ul style="list-style-type: none"> <li>containing toBeSigned <ul style="list-style-type: none"> <li>containing validityPeriod <ul style="list-style-type: none"> <li>containing start <ul style="list-style-type: none"> <li>indicating value X_START_VALIDITY (<math>X\_START\_VALIDITY \leq GEN\_TIME</math>)</li> </ul> </li> <li>and containing duration <ul style="list-style-type: none"> <li>indicating value <math>&gt; GEN\_TIME - X\_START\_VALIDITY</math></li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul>	

## 6.2.3.6 Check generation location

<b>TP Id</b>	TP_SEC_ITSS_SND_DENM_06_BV
<b>Summary</b>	Check that IUT sends the secured DENM containing generation location when signing certificate chain does not have any region restriction
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.2 IEEE Std 1609.2 [2], clause 5.2.3.2.2
<b>PICS Selection</b>	PICS_GN_SECURITY AND PICS_SEC_CERTIFICATE_SELECTION
<b>Expected behaviour</b>	
<p>with</p> <ul style="list-style-type: none"> <li>the IUT has been authorized with the AT certificate (CERT_IUT_A_AT) <ul style="list-style-type: none"> <li>containing toBeSigned <ul style="list-style-type: none"> <li>not containing region</li> </ul> </li> <li>and issued by the certificate AA (CERT_IUT_A_AA) <ul style="list-style-type: none"> <li>containing toBeSigned <ul style="list-style-type: none"> <li>not containing region</li> </ul> </li> <li>and issued by the certificate RCA (CERT_IUT_A_RCA) <ul style="list-style-type: none"> <li>containing toBeSigned <ul style="list-style-type: none"> <li>not containing region</li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> <p>ensure that</p> <ul style="list-style-type: none"> <li>when <ul style="list-style-type: none"> <li>the IUT is requested to send a secured DENM</li> </ul> </li> <li>then <ul style="list-style-type: none"> <li>the IUT sends a message of type EtsiTs103097Data <ul style="list-style-type: none"> <li>containing headerInfo <ul style="list-style-type: none"> <li>containing generationLocation</li> </ul> </li> </ul> </li> </ul> </li> </ul>	



<b>TP Id</b>	TP_SEC_ITSS_SND_DENM_07_BV_XX		
<b>Summary</b>	Check that IUT sends the secured DENM containing generation location which is inside the region defined by the validity restriction of the certificate pointed by the message signer		
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.2 IEEE Std 1609.2 [2], clause 5.2.3.2.2		
<b>PICS Selection</b>	PICS_GN_SECURITY AND PICS_SEC_CERTIFICATE_SELECTION AND <b>X_PICS</b>		
<b>Expected behaviour</b>			
with the IUT has been authorized with the AT certificate ( <b>X_AT_CERTIFICATE</b> ) containing toBeSigned containing region containing <b>X_FIELD</b> indicating REGION			
ensure that when the IUT is requested to send a secured DENM then the IUT sends a message of type EtsiTs103097Data containing headerInfo containing generationLocation indicating value inside the REGION			
<b>Permutation Table</b>			
<b>_XX</b>	<b>X_FIELD</b>	<b>X_AT_CERTIFICATE</b>	<b>X_PICS</b>
B	circularRegion	CERT_IUT_B_AT	PICS_SEC_CIRCULAR_REGION
C	rectangularRegion	CERT_IUT_C_AT	PICS_SEC_RECTANGULAR_REGION
D	polygonalRegion	CERT_IUT_D_AT	PICS_SEC_POLYGONAL_REGION
E	identifiedRegion	CERT_IUT_E_AT	PICS_SEC_IDENTIFIED_REGION

<b>TP Id</b>	TP_SEC_ITSS_SND_DENM_09_BV		
<b>Summary</b>	Check that IUT sends the secured DENM containing generation location which is inside the identified region defined by the validity restriction of the AA certificate used to sign the certificate pointed by the message signer does not contain any region restriction		
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.2 IEEE Std 1609.2 [2], clauses 5.2.3.2.2 and 6.4.8		
<b>PICS Selection</b>	PICS_GN_SECURITY AND PICS_SEC_CERTIFICATE_SELECTION		
<b>Expected behaviour</b>			
with the IUT has been authorized with the AT certificate (CERT_IUT_CA1_AT) containing toBeSigned not containing region and issued by the certificate AA (CERT_IUT_CC_AA) containing toBeSigned containing circularRegion indicating REGION and issued by the certificate RCA (CERT_IUT_C_RCA) containing toBeSigned containing circularRegion indicating REGION			
ensure that when the IUT is requested to send a secured DENM then the IUT sends a message of type EtsiTs103097Data containing headerInfo containing generationLocation indicating value inside the REGION			

<b>TP Id</b>	TP_SEC_ITSS_SND_DENM_10_BV
<b>Summary</b>	Check that IUT sends the secured DENM containing generation location which is inside the identified region defined by the validity restriction of the root certificate when subordinate AA and AT certificates do not contain any region restriction
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.2 IEEE Std 1609.2 [2], clauses 5.2.3.2.2 and 6.4.8
<b>PICS Selection</b>	PICS_GN_SECURITY AND PICS_SEC_CERTIFICATE_SELECTION
<b>Expected behaviour</b>	
<p>with</p> <ul style="list-style-type: none"> <li>the IUT has been authorized with the AT certificate (CERT_IUT_CA2_AT) <ul style="list-style-type: none"> <li>containing toBeSigned</li> <li>not containing region</li> </ul> </li> <li>and issued by the certificate AA (CERT_IUT_CA_AA) <ul style="list-style-type: none"> <li>containing toBeSigned</li> <li>not containing region</li> </ul> </li> <li>and issued by the certificate RCA (CERT_IUT_C_RCA) <ul style="list-style-type: none"> <li>containing toBeSigned</li> <li>containing circularRegion</li> <li>indicating REGION</li> </ul> </li> </ul> <p>ensure that</p> <ul style="list-style-type: none"> <li>when <ul style="list-style-type: none"> <li>the IUT is requested to send a secured DENM</li> </ul> </li> <li>then <ul style="list-style-type: none"> <li>the IUT sends a message of type EtsiTs103097Data <ul style="list-style-type: none"> <li>containing headerInfo <ul style="list-style-type: none"> <li>containing generationLocation</li> <li>indicating value inside the REGION</li> </ul> </li> </ul> </li> </ul> </li> </ul>	

### 6.2.3.7 Check payload

<b>TP Id</b>	TP_SEC_ITSS_SND_DENM_11_BV
<b>Summary</b>	Check that IUT sends the secured DENM containing the 'data' field in signed data payload, containing the EtsiTs103097Data of type unsecured, contained the DENM payload
<b>Reference</b>	ETSI TS 103 097 [1], clauses 5.2 and 7.1.2
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>with</p> <ul style="list-style-type: none"> <li>the IUT has been authorized with the AT certificate (CERT_IUT_A_AT)</li> </ul> <p>ensure that</p> <ul style="list-style-type: none"> <li>when <ul style="list-style-type: none"> <li>the IUT is requested to send a secured DENM</li> </ul> </li> <li>then <ul style="list-style-type: none"> <li>the IUT sends a message of type EtsiTs103097Data <ul style="list-style-type: none"> <li>contains content <ul style="list-style-type: none"> <li>contains signedData <ul style="list-style-type: none"> <li>containing tbsData <ul style="list-style-type: none"> <li>containing payload <ul style="list-style-type: none"> <li>containing data <ul style="list-style-type: none"> <li>containing content <ul style="list-style-type: none"> <li>containing unsecuredData <ul style="list-style-type: none"> <li>containing not-empty data</li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul>	

## 6.2.3.8 Check signing permissions

<b>TP Id</b>	TP_SEC_ITSS_SND_DENM_12_BV
<b>Summary</b>	Check that the IUT sends the secured DENM signed with the certificate containing appPermissions allowing to sign DEN messages
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.2 IEEE Std 1609.2 [2], clause 5.2.3.2.2
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>with  the IUT has been authorized with the AT certificate (CERT_IUT_A_AT)  ensure that  when  the IUT is requested to send a secured DENM  then  the IUT sends a message of type EtsiTs103097Data  containing signer  containing certificate  containing appPermissions  containing an item of type PsidSsp  containing psid  indicating AID_DENM</p>	

## 6.2.3.9 Check signature

<b>TP Id</b>	TP_SEC_ITSS_SND_DENM_13_BV			
<b>Summary</b>	Check that IUT sends the secured DENM containing signature Check that the signature is calculated over the right fields and using right hash algorithm by cryptographically verifying the signature			
<b>Reference</b>	ETSI TS 103 097 [1], clauses 5.2, 7.1.2 IEEE Std 1609.2 [2], clauses 5.3.1, 6.3.4, 6.3.29, 6.3.30 and 6.3.31			
<b>PICS Selection</b>	PICS_GN_SECURITY AND <b>X_PICS</b>			
<b>Expected behaviour</b>				
<p>with  the IUT is authorized with AT certificate (<b>X_CERTIFICATE</b>)  containing verifyKeyIndicator  containing verificationKey  containing <b>X_KEY</b>  indicating KEY</p> <p>ensure that  when  the IUT is requested to send a secured DENM  then  the IUT sends a message of type EtsiTs103097Data  containing signedData  containing signer  containing certificate  indicating <b>X_CERTIFICATE</b>  containing verifyKeyIndicator  containing verificationKey  containing <b>X_KEY</b>  indicating KEY  and containing signature  containing <b>X_SIGNATURE</b>  verifiable using KEY</p>				
<b>Permutation table</b>				
<b>XX</b>	<b>X_CERTIFICATE</b>	<b>X_KEY</b>	<b>X_SIGNATURE</b>	<b>X_PICS</b>
A	CERT_IUT_A_AT	ecdsaNistP256	ecdsaNistP256Signature	
B	CERT_IUT_A_B_AT	ecdsaBrainpoolP256r1	ecdsaBrainpoolP256r1Signature	PICS_SEC_BRAINPOOL_P256R1
C	CERT_IUT_A_B3_AT	ecdsaBrainpoolP384r1	ecdsaBrainpoolP384r1Signature	PICS_SEC_SHA384 AND PICS_SEC_BRAINPOOL_P384R1

## 6.2.3.10 Check support for certificate content

<b>TP Id</b>	TP_SEC_ITSS_SND_DENM_14_BV
<b>Summary</b>	Check that the IUT supports at least 8 entries in the rectangular certificate validity region in the AT certificate
<b>Reference</b>	IEEE Std 1609.2 [2], clause 6.4.17
<b>PICS Selection</b>	PICS_GN_SECURITY AND PICS_SEC_RECTANGULAR_REGION
<b>Expected behaviour</b>	
<p>with</p> <ul style="list-style-type: none"> <li>the IUT is authorized with AT certificate (CERT_IUT_C_AT_8) <ul style="list-style-type: none"> <li>containing toBeSigned</li> <li>containing region <ul style="list-style-type: none"> <li>containing rectangularRegion</li> <li>containing 8 entries <ul style="list-style-type: none"> <li>containing an entry (<b>ENTRY</b>)</li> <li>containing current IUT position</li> </ul> </li> </ul> </li> </ul> </li> </ul> <p>ensure that</p> <ul style="list-style-type: none"> <li>when <ul style="list-style-type: none"> <li>the IUT is requested to send a secured DENM</li> </ul> </li> <li>then <ul style="list-style-type: none"> <li>the IUT sends a message of type EtsiTs103097Data <ul style="list-style-type: none"> <li>containing headerInfo</li> <li>containing generationLocation</li> <li>indicating position inside the <b>ENTRY</b></li> </ul> </li> </ul> </li> </ul>	

<b>TP Id</b>	TP_SEC_ITSS_SND_DENM_15_BV
<b>Summary</b>	Check that the IUT supports at least 8 points in the polygonal certificate validity region in the AT certificate
<b>Reference</b>	IEEE Std 1609.2 [2], clause 6.4.17
<b>PICS Selection</b>	PICS_GN_SECURITY AND PICS_SEC_POLYGONAL_REGION
<b>Expected behaviour</b>	
<p>with</p> <ul style="list-style-type: none"> <li>the IUT is authorized with AT certificate (CERT_IUT_D_AT_8) <ul style="list-style-type: none"> <li>containing toBeSigned</li> <li>containing region <ul style="list-style-type: none"> <li>containing polygonalRegion</li> <li>containing 8 entries <ul style="list-style-type: none"> <li>indicating polygon <b>P</b></li> </ul> </li> </ul> </li> </ul> </li> <li>and the IUT's position is inside the polygon <b>P</b></li> </ul> <p>ensure that</p> <ul style="list-style-type: none"> <li>when <ul style="list-style-type: none"> <li>the IUT is requested to send a secured DENM</li> </ul> </li> <li>then <ul style="list-style-type: none"> <li>the IUT sends a message of type EtsiTs103097Data <ul style="list-style-type: none"> <li>containing headerInfo</li> <li>containing generationLocation</li> <li>indicating position inside the <b>P</b></li> </ul> </li> </ul> </li> </ul>	

<b>TP Id</b>	TP_SEC_ITSS_SND_DENM_16_BV
<b>Summary</b>	Check that the IUT supports at least 8 points in the polygonal certificate validity region in the AT certificate
<b>Reference</b>	IEEE Std 1609.2 [2], clause 6.4.17
<b>PICS Selection</b>	PICS_GN_SECURITY AND PICS_SEC_IDENTIFIED_REGION
<b>Expected behaviour</b>	
<p>with</p> <ul style="list-style-type: none"> <li>the IUT is authorized with AT certificate (CERT_IUT_E_AT_8) <ul style="list-style-type: none"> <li>containing toBeSigned</li> <li>containing region <ul style="list-style-type: none"> <li>containing identifiedRegion</li> <li>containing 8 entries <ul style="list-style-type: none"> <li>containing one of the items (<i>I</i>)</li> <li>containing current IUT position</li> </ul> </li> </ul> </li> </ul> </li> </ul> <p>ensure that</p> <ul style="list-style-type: none"> <li>when <ul style="list-style-type: none"> <li>the IUT is requested to send a secured DENM</li> </ul> </li> <li>then <ul style="list-style-type: none"> <li>the IUT sends a message of type EtsiTs103097Data <ul style="list-style-type: none"> <li>containing headerInfo</li> <li>containing generationLocation</li> <li>indicating position inside the <i>I</i></li> </ul> </li> </ul> </li> </ul>	

### 6.2.3.11 Check certificate consistency conditions

<b>TP Id</b>	TP_SEC_ITSS_SND_DENM_17_BV
<b>Summary</b>	Check that IUT does not send secured DENMs if IUT does not possess an AT certificate allowing sending messages in this location
<b>Reference</b>	IEEE Std 1609.2 [2], clause 6.2.3.2.2
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>with</p> <ul style="list-style-type: none"> <li>the IUT has been authorized with the AT certificate CERT_IUT_C1_AT) <ul style="list-style-type: none"> <li>containing region <ul style="list-style-type: none"> <li>indicating rectangular region</li> <li>not containing current IUT position</li> </ul> </li> </ul> </li> </ul> <p>ensure that</p> <ul style="list-style-type: none"> <li>when <ul style="list-style-type: none"> <li>the IUT is requested to send a secured DENM</li> </ul> </li> <li>then <ul style="list-style-type: none"> <li>the IUT does not send DENM</li> </ul> </li> </ul>	

<b>TP Id</b>	TP_SEC_ITSS_SND_DENM_18_BV
<b>Summary</b>	Check that IUT does not send the secured DENM if IUT is configured to use an AT certificate without region validity restriction and generation location is outside of the region of the issuing AA certificate
<b>Reference</b>	IEEE Std 1609.2 [2], clause 6.2.3.2.2
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>with</p> <ul style="list-style-type: none"> <li>the IUT has been authorized with the AT certificate (CERT_IUT_CA3_AT) <ul style="list-style-type: none"> <li>not containing region</li> <li>and issued by the AA certificate (CERT_IUT_C3_AA) <ul style="list-style-type: none"> <li>containing region <ul style="list-style-type: none"> <li>indicating rectangular region</li> <li>not containing current IUT position</li> </ul> </li> </ul> </li> </ul> </li> </ul> <p>ensure that</p> <ul style="list-style-type: none"> <li>when <ul style="list-style-type: none"> <li>the IUT is requested to send a secured DENM</li> </ul> </li> <li>then <ul style="list-style-type: none"> <li>the IUT does not send DENM</li> </ul> </li> </ul>	

<b>TP Id</b>	TP_SEC_ITSS_SND_DENM_19_BV
<b>Summary</b>	Check that IUT does not send secured DENMs if all AT certificates installed on the IUT are expired
<b>Reference</b>	IEEE Std 1609.2 [2], clause 6.2.3.2.2
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>with  the IUT is authorized with AT certificate (CERT_IUT_A1_AT)  containing validityPeriod  indicating start + duration &lt; CURRENT_TIME  and the IUT has no other installed AT certificates  ensure that  when  the IUT is requested to send a secured DENM  then  the IUT does not send DENM</p>	

<b>TP Id</b>	TP_SEC_ITSS_SND_DENM_20_BV
<b>Summary</b>	Check that IUT does not send secured DENMs if all AT certificates installed on the IUT have the starting time in the future
<b>Reference</b>	IEEE Std 1609.2 [2], clause 6.2.3.2.2
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>with  the IUT has been authorized with the AT certificate (CERT_IUT_A2_AT)  containing validityPeriod  indicating start &gt; CURRENT_TIME  and IUT has no other certificates installed  ensure that  when  the IUT is requested to send a secured DENM  then  the IUT does not send DENM</p>	

<b>TP Id</b>	TP_SEC_ITSS_SND_DENM_21_BV
<b>Summary</b>	Check that IUT does not send secured DENMs if IUT does not possess an AT certificate allowing sending DENM by its appPermissions
<b>Reference</b>	IEEE Std 1609.2 [2], clause 5.2.3.2.2
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>with  the IUT has been authorized with the AT certificate (CERT_IUT_A4_AT)  containing appPermissions  not containing PsidSSP  containing psid  indicating AID_DENM  and IUT has no other certificates installed  ensure that  when  the IUT is requested to send a secured DENM  then  the IUT does not send DENM</p>	

## 6.2.4 Generic signed message profile

### 6.2.4.1 Check that secured message is signed

<b>TP Id</b>	TP_SEC_ITSS_SND_GENMSG_01_BV
<b>Summary</b>	Check that IUT sends the secured message using signedData container
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.3
<b>PICS Selection</b>	PICS_GN_SECURITY AND PICS_SEC_ITS_AID_OTHER
<b>Expected behaviour</b>	
<p>with  the IUT is authorized with AT certificate (CERT_IUT_A_AT)  ensure that  when  the IUT is requested to send a secured Beacon  then  the IUT sends a message of type EtsiTs103097Data  containing content  containing signedData</p>	

### 6.2.4.2 Check secured AID value

<b>TP Id</b>	TP_SEC_ITSS_SND_GENMSG_02_BV
<b>Summary</b>	Check that the sent Secured Message contains HeaderField its_aid that is set to other value then AID_CAM and AID_DENM
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.3
<b>PICS Selection</b>	PICS_GN_SECURITY AND PICS_SEC_ITS_AID_OTHER
<b>Expected behaviour</b>	
<p>with  the IUT is authorized with AT certificate CERT_IUT_A_AT)  ensure that  when  the IUT is requested to send a secured Beacon  then  the IUT sends a message of type EtsiTs103097Data  containing content  containing signedData  containing tbsData  containing headerInfo  containing psid  indicating AID_GNMGMT</p>	

## 6.2.4.3 Check header field

<b>TP Id</b>	TP_SEC_ITSS_SND_GENMSG_03_BV
<b>Summary</b>	Check that IUT sends the secured GeoNetworking message with the headerInfo containing generationTime
<b>Reference</b>	ETSI TS 103 097 [1], clauses 5.2 and 7.1.3
<b>PICS Selection</b>	PICS_GN_SECURITY AND PICS_SEC_ITS_AID_OTHER
<b>Expected behaviour</b>	
<p>with  the IUT is authorized with AT certificate (CERT_IUT_A_AT)  ensure that  when  the IUT is requested to send a secured Beacon  then  the IUT sends a message of type EtsiTs103097Data  containing content  containing signedData  containing tbsData  containing headerInfo  containing generationTime  and not containing p2pcdLearningRequest  and not containing missingCrIIdentifier</p>	

## 6.2.4.4 Check that signer info is a certificate or digest

<b>TP Id</b>	TP_SEC_ITSS_SND_GENMSG_04_BV
<b>Summary</b>	Check that IUT sends the secured GeoNetworking message containing certificate or digest as a signer
<b>Reference</b>	ETSI TS 103 097 [1], clauses 5.2 and 7.1.3 IEEE Std 1609.2 [2], clause 6.3.4
<b>PICS Selection</b>	PICS_GN_SECURITY AND PICS_SEC_ITS_AID_OTHER
<b>Expected behaviour</b>	
<p>with  the IUT is authorized with AT certificate (CERT_IUT_A_AT)  ensure that  when  the IUT is requested to send a secured Beacon  then  the IUT sends a message of type EtsiTs103097Data  containing content  containing signedData  containing signer  containing digest  or containing certificate  containing toBeSigned  containing appPermissions  containing the item of type PsidSsp  containing psid  indicating AID_GNMGMT</p>	



## 6.2.4.5 Check generation time

<b>TP Id</b>	TP_SEC_ITSS_SND_GENMSG_05_BV
<b>Summary</b>	Check that IUT sends the secured GeoNetworking message containing generation time and this time is inside the validity period of the signing certificate Check that message generation time value is realistic
<b>Reference</b>	ETSI TS 103 097 [1], clauses 5.4 and 7.1.3
<b>PICS Selection</b>	PICS_GN_SECURITY AND PICS_SEC_ITS_AID_OTHER
<b>Expected behaviour</b>	
<p>with  the IUT is authorized with AT certificate (CERT_IUT_A_AT)  ensure that  when  the IUT is requested to send a secured Beacon  containing certificate  then  the IUT sends a message of type EtsiTs103097Data  containing headerInfo  containing generationTime  indicating GEN_TIME (CUR_TIME - 10 min &lt;= GEN_TIME &lt;= CUR_TIME + 10 min)  and containing signer  containing certificate  containing toBeSigned  containing validityPeriod  containing start  indicating value X_START_VALIDITY (X_START_VALIDITY &lt;= GEN_TIME)  and containing duration  indicating value &gt; GEN_TIME - X_START_VALIDITY</p>	

## 6.2.4.6 Check payload

<b>TP Id</b>	TP_SEC_ITSS_SND_GENMSG_06_BV
<b>Summary</b>	Check that IUT sends the secured message using the 'data' field in signed data payload, containing the EtsiTs103097Data of type unsecured, containing the data payload or using the extDataHash field containing the SHA256 hash of data payload
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.3
<b>PICS Selection</b>	PICS_GN_SECURITY AND PICS_SEC_ITS_AID_OTHER
<b>Expected behaviour</b>	
<p>with  the IUT is authorized with AT certificate (CERT_IUT_A_AT)  ensure that  when  the IUT is requested to send a secured Beacon  then  the IUT sends a message of type EtsiTs103097Data  contains content  contains signedData  containing tbsData  containing payload  containing data  containing content  containing unsecuredData  containing not-empty data</p>	

## 6.2.4.7 Check signing permissions

<b>TP Id</b>	TP_SEC_ITSS_SND_GENMSG_07_BV
<b>Summary</b>	Check that the IUT sends the secured messages signed with the certificate containing appPermissions allowing to sign these messages
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.3 IEEE Std 1609.2 [2], clause 5.2.3.2.2
<b>PICS Selection</b>	PICS_GN_SECURITY AND PICS_SEC_ITS_AID_OTHER
<b>Expected behaviour</b>	
<p>with  the IUT has been authorized with the AT certificate (CERT_IUT_A_AT)  ensure that  when  the IUT is requested to send Beacon  then  the IUT sends a message of type EtsiTs103097Data  containing signer  containing certificate  containing appPermissions  containing an item of type PsidSsp  containing psid  indicating value AID_GNMGMT</p>	

## 6.2.4.8 Check signature

<b>TP Id</b>	TP_SEC_ITSS_SND_GENMSG_08_BV			
<b>Summary</b>	Check that IUT sends the secured GeoNetworking message containing signature Check that the signature is calculated over the right fields and using right hash algorithm by <u>cryptographically verifying the signature</u>			
<b>Reference</b>	ETSI TS 103 097 [1], clauses 5.2 and 7.1.3 IEEE Std 1609.2 [2], clauses 5.3.1, 6.3.4, 6.3.29, 6.3.30 and 6.3.31			
<b>PICS Selection</b>	PICS_GN_SECURITY AND PICS_SEC_ITS_AID_OTHER AND <b>X_PICS</b>			
<b>Expected behaviour</b>				
<p>with  the IUT is authorized with AT certificate (<b>X_CERTIFICATE</b>)  containing verifyKeyIndicator  containing verificationKey  containing <b>X_KEY</b>  indicating KEY</p> <p>ensure that  when  the IUT is requested to send a secured Beacon  then  the IUT sends a message of type EtsiTs103097Data  containing signedData  containing signer  containing digest  referencing the certificate <b>X_CERTIFICATE</b>  or containing certificate  indicating <b>X_CERTIFICATE</b>  and containing signature  containing <b>X_SIGNATURE</b>  verifiable using KEY</p>				
<b>Permutation table</b>				
<b>XX</b>	<b>X_CERTIFICATE</b>	<b>X_KEY</b>	<b>X_SIGNATURE</b>	<b>X_PICS</b>
A	CERT_IUT_A_AT	ecdsaNistP256	ecdsaNistP256Signature	
B	CERT_IUT_A_B_AT	ecdsaBrainpoolP256r1	ecdsaBrainpoolP256r1Signature	PICS_SEC_BRAINPOOL_P 256R1
C	CERT_IUT_A_B3_AT	ecdsaBrainpoolP384r1	ecdsaBrainpoolP384r1Signature	PICS_SEC_SHA384 AND PICS_SEC_BRAINPOOL_P 384R1

## 6.3 Receiving behaviour

### 6.3.1 Check the message protocol version

<b>TP Id</b>	TP_SEC_ITSS_RCV_MSG_01_BV
<b>Summary</b>	Check that IUT accepts a secured message containing protocol version set to a value 3
<b>Reference</b>	ETSI TS 103 097 [1], clause 5.1
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>with</p> <ul style="list-style-type: none"> <li>the IUT is being authorized with the certificate CERT_IUT_A_AT</li> <li>and the IUT current time is inside the time validity period of CERT_TS_A_AT and CERT_IUT_A_AT</li> </ul> <p>ensure that</p> <ul style="list-style-type: none"> <li>when           <ul style="list-style-type: none"> <li>the IUT is receiving a message of type EtsiTs103097Data</li> <li>signed using CERT_TS_A_AT</li> <li>and containing protocolVersion</li> <li>indicating 3</li> </ul> </li> <li>then           <ul style="list-style-type: none"> <li>the IUT forwards the SecuredMessage to the Facility layers</li> </ul> </li> </ul>	

<b>TP Id</b>	TP_SEC_ITSS_RCV_MSG_01_BO
<b>Summary</b>	Check that IUT discards a secured message containing protocol version set to a value less than 3
<b>Reference</b>	ETSI TS 103 097 [1], clause 5.1
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>with</p> <ul style="list-style-type: none"> <li>the IUT is being authorized with the certificate CERT_IUT_A_AT</li> <li>and the IUT current time is inside the time validity period of CERT_TS_A_AT and CERT_IUT_A_AT</li> </ul> <p>ensure that</p> <ul style="list-style-type: none"> <li>when           <ul style="list-style-type: none"> <li>the IUT is receiving a message of type EtsiTs103097Data</li> <li>signed using CERT_TS_A_AT</li> <li>and containing protocolVersion</li> <li>indicating 2</li> </ul> </li> <li>then           <ul style="list-style-type: none"> <li>the IUT discards the SecuredMessage</li> </ul> </li> </ul>	

<b>TP Id</b>	TP_SEC_ITSS_RCV_MSG_02_BO
<b>Summary</b>	Check that IUT discards a secured message containing protocol version set to a value greater than 3
<b>Reference</b>	ETSI TS 103 097 [1], clause 5.1
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>with</p> <ul style="list-style-type: none"> <li>the IUT is being authorized with the certificate CERT_IUT_A_AT</li> <li>and the IUT current time is inside the time validity period of CERT_TS_A_AT and CERT_IUT_A_AT</li> </ul> <p>ensure that</p> <ul style="list-style-type: none"> <li>when           <ul style="list-style-type: none"> <li>the IUT is receiving a message of type EtsiTs103097Data</li> <li>signed using CERT_TS_A_AT</li> <li>and containing protocolVersion</li> <li>indicating 4</li> </ul> </li> <li>then           <ul style="list-style-type: none"> <li>the IUT discards the SecuredMessage</li> </ul> </li> </ul>	

## 6.3.2 CAM profile

### 6.3.2.1 Check the valid message receiving

<b>TP Id</b>	TP_SEC_ITSS_RCV_CAM_01_BV
<b>Summary</b>	Check that IUT accepts a valid secured CAM message signed with certificate
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.1
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>with</p> <ul style="list-style-type: none"> <li>the IUT being in the 'authorized' state</li> <li>and the IUT current time (CUR_TIME) is inside the time validity period of CERT_TS_A_AT</li> </ul> <p>ensure that</p> <ul style="list-style-type: none"> <li>when           <ul style="list-style-type: none"> <li>the IUT is receiving a message of type EtsiTs103097Data (MSG)               <ul style="list-style-type: none"> <li>containing protocolVersion                   <ul style="list-style-type: none"> <li>indicating 3</li> </ul> </li> <li>and containing content.signedData                   <ul style="list-style-type: none"> <li>containing hashId                       <ul style="list-style-type: none"> <li>indicating hash algorithm of the verification key of CERT_TS_A_AT</li> </ul> </li> <li>and containing tbsData                       <ul style="list-style-type: none"> <li>containing payload                           <ul style="list-style-type: none"> <li>containing data                               <ul style="list-style-type: none"> <li>containing protocolVersion                                   <ul style="list-style-type: none"> <li>indicating 3</li> </ul> </li> <li>and containing content.unsecuredData                                   <ul style="list-style-type: none"> <li>containing CAM payload</li> </ul> </li> </ul> </li> <li>and containing headerInfo                       <ul style="list-style-type: none"> <li>containing psid                           <ul style="list-style-type: none"> <li>indicating CAM AID value</li> </ul> </li> <li>and containing generationTime                           <ul style="list-style-type: none"> <li>indicating time within 2sec around the CUR_TIME</li> </ul> </li> <li>and NOT containing other headers</li> </ul> </li> <li>and containing signer                       <ul style="list-style-type: none"> <li>containing certificate                           <ul style="list-style-type: none"> <li>containing 1 item of type EtsiTs103097Certificate                               <ul style="list-style-type: none"> <li>indicating CERT_TS_A_AT</li> </ul> </li> </ul> </li> <li>and containing signature                       <ul style="list-style-type: none"> <li>containing ecdsaNistP256Signature                           <ul style="list-style-type: none"> <li>containing rSig.x-only                               <ul style="list-style-type: none"> <li>calculated over the MSG.content.signedData.tbsData</li> </ul> </li> <li>using verification key of CERT_TS_A_AT</li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> <p>then</p> <ul style="list-style-type: none"> <li>the IUT accepts the SecuredMessage</li> </ul> </li></ul></li></ul></li></ul>	

<b>TP Id</b>	TP_SEC_ITSS_RCV_CAM_02_BV
<b>Summary</b>	Check that IUT accepts a valid secured CAM message signed with digest
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.1
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>with</p> <ul style="list-style-type: none"> <li>the IUT being in the 'authorized' state</li> <li>and the IUT current time (CUR_TIME) is inside the time validity period of CERT_TS_A_AT</li> <li>and the IUT has already received the message signed with CERT_TS_A_AT</li> </ul> <p>ensure that</p> <ul style="list-style-type: none"> <li>when           <ul style="list-style-type: none"> <li>the IUT is receiving a message of type EtsiTs103097Data               <ul style="list-style-type: none"> <li>indicating the message described in TP_SEC_ITSS_RCV_CAM_01_BV</li> <li>and containing content.signedData.signer                   <ul style="list-style-type: none"> <li>containing digest                       <ul style="list-style-type: none"> <li>indicating HashedId8 value                           <ul style="list-style-type: none"> <li>referencing the CERT_TS_A_AT</li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> <p>then</p> <ul style="list-style-type: none"> <li>the IUT accepts the SecuredMessage</li> </ul> </li></ul>	

<b>TP Id</b>	TP_SEC_ITSS_RCV_CAM_03_BV
<b>Summary</b>	Check that IUT accepts a valid secured CAM message signed with compressed signature
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.1
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>with  the IUT being in the 'authorized' state  and the IUT current time (CUR_TIME) is inside the time validity period of CERT_TS_A_AT</p> <p>ensure that  when  the IUT is receiving a message of type EtsiTs103097Data (MSG)  indicating the message described in TP_SEC_ITSS_RCV_CAM_01_BV  and containing content.signedData.signature  containing ecdsaNistP256Signature  containing rSig.compressed-y-0  or containing rSig.compressed-y-1  calculated over the MSG.content.signedData.tbsData  using verification key of CERT_TS_A_AT</p> <p>then  the IUT accepts the SecuredMessage</p>	

<b>TP Id</b>	TP_SEC_ITSS_RCV_CAM_04_BV_XX		
<b>Summary</b>	Check that IUT accepts a valid secured CAM message signed with certificate containing region restriction		
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.1		
<b>PICS Selection</b>	PICS_GN_SECURITY AND <b>X_PICS</b>		
<b>Expected behaviour</b>			
<p>with  the IUT being in the 'authorized' state  and the IUT current time (CUR_TIME) is inside the time validity period of <b>X_AT_CERTIFICATE</b>  and the IUT current position is inside the region restriction of <b>X_AT_CERTIFICATE</b></p> <p>ensure that  when  the IUT is receiving a message of type EtsiTs103097Data (MSG)  indicating the message described in TP_SEC_ITSS_RCV_CAM_01_BV  and containing content.signedData  containing signer  containing certificate  containing 1 item of type EtsiTs103097Certificate  indicating <b>X_AT_CERTIFICATE</b>  containing toBeSigned.region  containing <b>X_FIELD</b></p> <p>and containing signature  containing ecdsaNistP256Signature  containing rSig.x-only  calculated over the MSG.content.signedData.tbsData  using verification key of <b>X_AT_CERTIFICATE</b></p> <p>then  the IUT accepts the SecuredMessage</p>			
<b>Permutation Table</b>			
<b>XX</b>	<b>X_FIELD</b>	<b>X_AT_CERTIFICATE</b>	<b>X_PICS</b>
01	circularRegion	CERT_TS_B_AT	PICS_SEC_CIRCULAR_REGION
02	rectangularRegion	CERT_TS_C_AT	PICS_SEC_RECTANGULAR_REGION
03	polygonalRegion	CERT_TS_D_AT	PICS_SEC_POLYGONAL_REGION
04	identifiedRegion	CERT_TS_E_AT	PICS_SEC_IDENTIFIED_REGION

<b>TP Id</b>	TP_SEC_ITSS_RCV_CAM_05_BV
<b>Summary</b>	Check that IUT accepts a valid secured CAM message signed using the brainpoolP256r1 algorithm
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.1
<b>PICS Selection</b>	PICS_GN_SECURITY AND PICS_SEC_BRAINPOOL_P256R1
<b>Expected behaviour</b>	
<p>With  the IUT being in the 'authorized' state  and the IUT current time (CUR_TIME) is inside the time validity period of CERT_TS_A_B_AT  ensure that  when  the IUT is receiving a message of type EtsiTs103097Data  indicating the message described in TP_SEC_ITSS_RCV_CAM_01_BV  and containing content.signedData  containing signer  containing certificate  containing 1 item of type EtsiTs103097Certificate  indicating CERT_TS_A_B_AT  containing toBeSigned.verifyKeyIndicator.verificationKey  containing ecdsaBrainpoolP256r1  and containing signature  containing ecdsaBrainpoolP256r1Signature  containing rSig.x-only  calculated over the MSG.content.signedData.tbsData  using verification key of CERT_TS_A_B_AT  then  the IUT accepts the SecuredMessage</p>	

<b>TP Id</b>	TP_SEC_ITSS_RCV_CAM_06_BV
<b>Summary</b>	Check that IUT accepts a valid secured CAM message signed using the brainpoolP384r1 algorithm
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.1
<b>PICS Selection</b>	PICS_GN_SECURITY AND PICS_SEC_BRAINPOOL_P384R1
<b>Expected behaviour</b>	
<p>With  the IUT being in the 'authorized' state  and the IUT current time (CUR_TIME) is inside the time validity period of CERT_TS_A_B3_AT  ensure that  when  the IUT is receiving a message of type EtsiTs103097Data  indicating the message described in TP_SEC_ITSS_RCV_CAM_01_BV  and containing content.signedData  containing signer  containing certificate  containing 1 item of type EtsiTs103097Certificate  indicating CERT_TS_A_B3_AT  containing toBeSigned.verifyKeyIndicator.verificationKey  containing ecdsaBrainpoolP384r1  and containing signature  containing ecdsaBrainpoolP384r1Signature  containing rSig.x-only  calculated over the MSG.content.signedData.tbsData  using verification key of CERT_TS_A_B3_AT  then  the IUT accepts the SecuredMessage</p>	

## 6.3.2.2 Check invalid HeaderInfo elements

<b>TP Id</b>	TP_SEC_ITSS_RCV_CAM_01_BO
<b>Summary</b>	Check that IUT discards a secured CAM if the HeaderInfo contains the header field an invalid Psid value
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.1
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>with  the IUT being in the 'authorized' state  and the IUT current time is inside the time validity period of CERT_TS_A_AT  ensure that  when  the IUT is receiving a message of type EtsiTs103097Data  indicating the message described in TP_SEC_ITSS_RCV_CAM_02_BV  and containing SignedData  containing ToBeSignedData  containing HeaderInfo  containing psid  <b>not</b> indicating CAM AID value  then  the IUT discards the SecuredMessage</p>	

<b>TP Id</b>	TP_SEC_ITSS_RCV_CAM_02_BO
<b>Summary</b>	Check that IUT discards a secured CAM if the HeaderInfo contains the header field generationLocation
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.1
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>With  the IUT being in the 'authorized' state  and the IUT current time is inside the time validity period of CERT_TS_A_AT  ensure that  when  the IUT is receiving a message of type EtsiTs103097Data  containing SignedData  containing ToBeSignedData  containing HeaderInfo  containing psid  indicating CAM AID value  and containing generationLocation  then  the IUT discards the SecuredMessage</p>	

<b>TP Id</b>	TP_SEC_ITSS_RCV_CAM_03_BO
<b>Summary</b>	Check that IUT discards a secured CAM if the HeaderInfo contains the header field expiryTime
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.1
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>With  the IUT being in the 'authorized' state  and the IUT current time is inside the time validity period of CERT_TS_A_AT  ensure that  when  the IUT is receiving a message of type EtsiTs103097Data  containing SignedData  containing ToBeSignedData  containing HeaderInfo  containing psid  indicating CAM AID value  and containing expiryTime  then  the IUT discards the SecuredMessage</p>	

<b>TP Id</b>	TP_SEC_ITSS_RCV_CAM_04_BO
<b>Summary</b>	Check that IUT discards a secured CAM if the HeaderInfo contains the header field p2pcdLearningRequest
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.1
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>With  the IUT being in the 'authorized' state  and the IUT current time is inside the time validity period of CERT_TS_A_AT  ensure that  when  the IUT is receiving a message of type EtsiTs103097Data  containing SignedData  containing ToBeSignedData  containing HeaderInfo  containing psid  indicating CAM AID value  and containing p2pcdLearningRequest  then  the IUT discards the SecuredMessage</p>	

<b>TP Id</b>	TP_SEC_ITSS_RCV_CAM_05_BO
<b>Summary</b>	Check that IUT discards a secured CAM if the HeaderInfo contains the header field missingCrIIdentifier
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.1
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>With  the IUT being in the 'authorized' state  and the IUT current time is inside the time validity period of CERT_TS_A_AT  ensure that  when  the IUT is receiving a message of type EtsiTs103097Data  containing SignedData  containing ToBeSignedData  containing HeaderInfo  containing psid  indicating CAM AID value  and containing missingCrIIdentifier  then  the IUT discards the SecuredMessage</p>	



<b>TP Id</b>	TP_SEC_ITSS_RCV_CAM_06_BO
<b>Summary</b>	Check that IUT discards a secured CAM if the HeaderInfo contains the header field encryptionKey
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.1
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>With  the IUT being in the 'authorized' state  and the IUT current time is inside the time validity period of CERT_TS_A_AT  ensure that  when  the IUT is receiving a message of type EtsiTs103097Data  containing SignedData  containing ToBeSignedData  containing HeaderInfo  containing psid  indicating CAM AID value  and containing encryptionKey  then  the IUT discards the SecuredMessage</p>	

### 6.3.2.3 Check invalid Signature elements

<b>TP Id</b>	TP_SEC_ITSS_RCV_CAM_07_BO
<b>Summary</b>	Check that IUT discards a secured CAM if the 'SignedData' contains an invalid signature algorithm
<b>Reference</b>	ETSI TS 103 097 [1], clause 6
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>with  the IUT being in the 'authorized' state  and the IUT current time is inside the time validity period of CERT_TS_A_AT  ensure that  when  the IUT is receiving a message of type EtsiTs103097Data  containing SignedData  containing Signature  indicating invalid signature algorithm  then  the IUT discards the SecuredMessage</p>	

<b>TP Id</b>	TP_SEC_ITSS_RCV_CAM_08_BO
<b>Summary</b>	Check that IUT discards a secured CAM if the 'SignerIdentifier' contains an invalid choice
<b>Reference</b>	ETSI TS 103 097 [1], clause 6
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>with  the IUT being in the 'authorized' state  and the IUT current time is inside the time validity period of CERT_TS_A_AT  ensure that  when  the IUT is receiving a message of type EtsiTs103097Data  containing SignedData  containing SignerIdentifier  indicating 'self'  then  the IUT discards the SecuredMessage</p>	

<b>TP Id</b>	TP_SEC_ITSS_RCV_CAM_09_BO
<b>Summary</b>	Check that IUT discards a secured CAM if the Signature cannot be verified
<b>Reference</b>	ETSI TS 103 097 [1], clause 6
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>with  the IUT being in the 'authorized' state  and the IUT current time is inside the time validity period of CERT_TS_A_AT  ensure that  when  the IUT is receiving a message of type EtsiTs103097Data  containing Signature  indicating an altered value  different then the one calculated using signature calculated rules  then  the IUT discards the SecuredMessage</p>	

### 6.3.3 DENM profile

#### 6.3.3.1 Check the valid message receiving

<b>TP Id</b>	TP_SEC_ITSS_RCV_DENM_01_BV
<b>Summary</b>	Check that IUT accepts a valid secured DENM message signed with certificate
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.1
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>with  the IUT being in the 'authorized' state  and the IUT current time (CUR_TIME) is inside the time validity period of CERT_TS_A_AT  ensure that  when  the IUT is receiving a message of type EtsiTs103097Data (MSG)  containing protocolVersion  indicating 3  and containing content.signedData  containing hashId  indicating hash algorithm of the verification key of CERT_TS_A_AT  and containing tbsData  containing payload  containing data  containing protocolVersion  indicating 3  and containing content.unsecuredData  containing DENM payload  and containing headerInfo  containing psid  indicating DENM AID value  and containing generationTime  indicating time within 2sec around the CUR_TIME  and containing generationLocation  and NOT containing other headers  and containing signer  containing certificate  containing 1 item of type EtsiTs103097Certificate  indicating CERT_TS_A_AT  and containing signature  containing ecdsaNistP256Signature  containing rSig.x-only  calculated over the MSG.content.signedData.tbsData  using verification key of CERT_TS_A_AT  then  the IUT accepts the SecuredMessage</p>	

<b>TP Id</b>	TP_SEC_ITSS_RCV_DENM_02_BV_XX		
<b>Summary</b>	Check that IUT accepts a valid secured DENM message signed with certificate containing region restriction		
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.1		
<b>PICS Selection</b>	PICS_GN_SECURITY AND <b>X_PICS</b>		
<b>Expected behaviour</b>			
<p>with</p> <ul style="list-style-type: none"> <li>the IUT being in the 'authorized' state</li> <li>and the IUT current time (CUR_TIME) is inside the time validity period of <b>X_AT_CERTIFICATE</b></li> <li>and the IUT current position is inside the region restriction of <b>X_AT_CERTIFICATE</b></li> </ul> <p>ensure that</p> <ul style="list-style-type: none"> <li>when <ul style="list-style-type: none"> <li>the IUT is receiving a message of type EtsiTs103097Data (MSG) <ul style="list-style-type: none"> <li>indicating the message described in TP_SEC_ITSS_RCV_DENM_01_BV</li> <li>and containing content.signedData <ul style="list-style-type: none"> <li>containing tbsData <ul style="list-style-type: none"> <li>containing headerInfo <ul style="list-style-type: none"> <li>containing generationLocation <ul style="list-style-type: none"> <li>indicating location inside the <b>X_AT_CERTIFICATE</b> region restriction</li> </ul> </li> </ul> </li> <li>and containing signer <ul style="list-style-type: none"> <li>containing certificate <ul style="list-style-type: none"> <li>containing 1 item of type EtsiTs103097Certificate <ul style="list-style-type: none"> <li>indicating <b>X_AT_CERTIFICATE</b> <ul style="list-style-type: none"> <li>containing toBeSigned.region <ul style="list-style-type: none"> <li>containing <b>X_FIELD</b></li> </ul> </li> </ul> </li> <li>and containing signature <ul style="list-style-type: none"> <li>containing ecdsaNistP256Signature <ul style="list-style-type: none"> <li>containing rSig.x-only <ul style="list-style-type: none"> <li>calculated over the MSG.content.signedData.tbsData <ul style="list-style-type: none"> <li>using verification key of <b>X_AT_CERTIFICATE</b></li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> <p>then</p> <ul style="list-style-type: none"> <li>the IUT accepts the SecuredMessage</li> </ul> </li></ul>			
<b>Permutation Table</b>			
<b>_XX</b>	<b>X_FIELD</b>	<b>X_AT_CERTIFICATE</b>	<b>X_PICS</b>
01	circularRegion	CERT_TS_B_AT	PICS_SEC_CIRCULAR_REGION
02	rectangularRegion	CERT_TS_C_AT	PICS_SEC_RECTANGULAR_REGION
03	polygonalRegion	CERT_TS_D_AT	PICS_SEC_POLYGONAL_REGION
04	identifiedRegion	CERT_TS_E_AT	PICS_SEC_IDENTIFIED_REGION

<b>TP Id</b>	TP_SEC_ITSS_RCV_DENM_03_BV
<b>Summary</b>	Check that IUT accepts a valid secured DENM message signed using the brainpoolP256r1 algorithm
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.1
<b>PICS Selection</b>	PICS_GN_SECURITY AND PICS_SEC_BRAINPOOL_P256R1
<b>Expected behaviour</b>	
<p>With  the IUT being in the 'authorized' state  and the IUT current time (CUR_TIME) is inside the time validity period of CERT_TS_A_B_AT  ensure that  when  the IUT is receiving a message of type EtsiTs103097Data (MSG)  indicating the message described in TP_SEC_ITSS_RCV_DENM_01_BV  and containing content.signedData  containing signer  containing certificate  containing 1 item of type EtsiTs103097Certificate  indicating CERT_TS_A_B_AT  containing toBeSigned.verifyKeyIndicator.verificationKey  containing ecdsaBrainpoolP256r1  and containing signature  containing ecdsaBrainpoolP256r1Signature  containing rSig.x-only  calculated over the MSG.content.signedData.tbsData  using verification key of CERT_TS_A_B_AT  then  the IUT accepts the SecuredMessage</p>	

<b>TP Id</b>	TP_SEC_ITSS_RCV_DENM_04_BV
<b>Summary</b>	Check that IUT accepts a valid secured DENM message signed using the brainpoolP384r1 algorithm
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.1
<b>PICS Selection</b>	PICS_GN_SECURITY AND PICS_SEC_BRAINPOOL_P384R1
<b>Expected behaviour</b>	
<p>With  the IUT being in the 'authorized' state  and the IUT current time (CUR_TIME) is inside the time validity period of CERT_TS_A_B3_AT  ensure that  when  the IUT is receiving a message of type EtsiTs103097Data (MSG)  indicating the message described in TP_SEC_ITSS_RCV_DENM_01_BV  and containing content.signedData  containing signer  containing certificate  containing 1 item of type EtsiTs103097Certificate  indicating CERT_TS_A_B3_AT  containing toBeSigned.verifyKeyIndicator.verificationKey  containing ecdsaBrainpoolP384r1  and containing signature  containing ecdsaBrainpoolP384r1Signature  containing rSig.x-only  calculated over the MSG.content.signedData.tbsData  using verification key of CERT_TS_A_B3_AT  then  the IUT accepts the SecuredMessage</p>	

## 6.3.3.2 Check invalid HeaderInfo elements

<b>TP Id</b>	TP_SEC_ITSS_RCV_DENM_01_BO
<b>Summary</b>	Check that IUT discards a secured DENM if the HeaderInfo contains the header field an invalid Psid value
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.2
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>With  the IUT being in the 'authorized' state  and the IUT current time is inside the time validity period of CERT_TS_A_AT  ensure that  when  the IUT is receiving a message of type EtsiTs103097Data  containing SignedData  containing ToBeSignedData  containing HeaderInfo  containing psid  <b>not</b> indicating DENM AID value  then  the IUT discards the SecuredMessage</p>	

<b>TP Id</b>	TP_SEC_ITSS_RCV_DENM_02_BO
<b>Summary</b>	Check that IUT discards a secured DENM if the HeaderInfo does not contain the header field generationLocation
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.2
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>With  the IUT being in the 'authorized' state  and the IUT current time is inside the time validity period of CERT_TS_A_AT  ensure that  when  the IUT is receiving a message of type EtsiTs103097Data  containing SignedData  containing ToBeSignedData  containing HeaderInfo  containing Psid  indicating DENM AID value  and <b>not</b> containing generationLocation  then  the IUT discards the SecuredMessage</p>	

<b>TP Id</b>	TP_SEC_ITSS_RCV_DENM_03_BO
<b>Summary</b>	Check that IUT discards a secured DENM if the HeaderInfo contains the header field expiryTime
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.2
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>With  the IUT being in the 'authorized' state  and the IUT current time is inside the time validity period of CERT_TS_A_AT  ensure that  when  the IUT is receiving a message of type EtsiTs103097Data  containing SignedData  containing ToBeSignedData  containing HeaderInfo  containing Psid  indicating DENM AID value  and containing expiryTime  then  the IUT discards the SecuredMessage</p>	

<b>TP Id</b>	TP_SEC_ITSS_RCV_DENM_04_BO
<b>Summary</b>	Check that IUT discards a secured DENM if the HeaderInfo contains the header field p2pcdLearningRequest
<b>Reference</b>	ETSI TS 103 097 [1], clause 5.2
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>With  the IUT being in the 'authorized' state  and the IUT current time is inside the time validity period of CERT_TS_A_AT  ensure that  when  the IUT is receiving a message of type EtsiTs103097Data  containing SignedData  containing ToBeSignedData  containing HeaderInfo  containing Psid  indicating DENM AID value  and containing p2pcdLearningRequest  then  the IUT discards the SecuredMessage</p>	

<b>TP Id</b>	TP_SEC_ITSS_RCV_DENM_05_BO
<b>Summary</b>	Check that IUT discards a secured DENM if the HeaderInfo contains the header field missingCrIIdentifier
<b>Reference</b>	ETSI TS 103 097 [1], clause 5.2
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>With  the IUT being in the 'authorized' state  and the IUT current time is inside the time validity period of CERT_TS_A_AT  ensure that  when  the IUT is receiving a message of type EtsiTs103097Data  containing SignedData  containing ToBeSignedData  containing HeaderInfo  containing Psid  indicating DENM AID value  and containing missingCrIIdentifier  then  the IUT discards the SecuredMessage</p>	

<b>TP Id</b>	TP_SEC_ITSS_RCV_DENM_06_BO
<b>Summary</b>	Check that IUT discards a secured DENM if the HeaderInfo contains the header field encryptionKey
<b>Reference</b>	ETSI TS 103 097 [1], clause 7.1.2
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>With  the IUT being in the 'authorized' state  and the IUT current time is inside the time validity period of CERT_TS_A_AT  ensure that  when  the IUT is receiving a message of type EtsiTs103097Data  containing SignedData  containing ToBeSignedData  containing HeaderInfo  containing Psid  indicating DENM AID value  and containing encryptionKey  then  the IUT discards the SecuredMessage</p>	

## 6.3.3.3 Check invalid Signature elements

<b>TP Id</b>	TP_SEC_ITSS_RCV_DENM_07_BO
<b>Summary</b>	Check that IUT discards a secured DENM if the 'SignedData' contains an invalid signature algorithm
<b>Reference</b>	ETSI TS 103 097 [1], clause 6
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>with</p> <ul style="list-style-type: none"> <li>the IUT being in the 'authorized' state</li> <li>and the IUT current time is inside the time validity period of CERT_TS_A_AT</li> </ul> <p>ensure that</p> <ul style="list-style-type: none"> <li>when <ul style="list-style-type: none"> <li>the IUT is receiving a message of type EtsiTs103097Data containing SignedData containing Signature indicating invalid signature algorithm</li> </ul> </li> <li>then <ul style="list-style-type: none"> <li>the IUT discards the SecuredMessage</li> </ul> </li> </ul>	

<b>TP Id</b>	TP_SEC_ITSS_RCV_DENM_08_BO
<b>Summary</b>	Check that IUT discards a secured DENM if the 'SignerIdentifier' contains an invalid choice
<b>Reference</b>	ETSI TS 103 097 [1], clause 6
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>with</p> <ul style="list-style-type: none"> <li>the IUT being in the 'authorized' state</li> <li>and the IUT current time is inside the time validity period of CERT_TS_A_AT</li> </ul> <p>ensure that</p> <ul style="list-style-type: none"> <li>when <ul style="list-style-type: none"> <li>the IUT is receiving a message of type EtsiTs103097Data containing SignedData containing SignerIdentifier indicating 'self'</li> </ul> </li> <li>then <ul style="list-style-type: none"> <li>the IUT discards the SecuredMessage</li> </ul> </li> </ul>	

<b>TP Id</b>	TP_SEC_ITSS_RCV_DENM_09_BO
<b>Summary</b>	Check that IUT discards a secured DENM if the Signature cannot be verified
<b>Reference</b>	ETSI TS 103 097 [1], clause 6
<b>PICS Selection</b>	PICS_GN_SECURITY
<b>Expected behaviour</b>	
<p>with</p> <ul style="list-style-type: none"> <li>the IUT being in the 'authorized' state</li> <li>and the IUT current time is inside the time validity period of CERT_TS_A_AT</li> </ul> <p>ensure that</p> <ul style="list-style-type: none"> <li>when <ul style="list-style-type: none"> <li>the IUT is receiving a message of type EtsiTs103097Data containing Signature indicating an altered value different from the one calculated using the signature calculation rules</li> </ul> </li> <li>then <ul style="list-style-type: none"> <li>the IUT discards the SecuredMessage</li> </ul> </li> </ul>	

---

## Annex A (informative): Bibliography

- ETSI TS 102 894-2 (V1.2.1): "Intelligent Transport Systems (ITS); Users and applications requirements; Part 2: Applications and facilities layer common data dictionary".



---

## History

<b>Document history</b>		
V1.1.1	July 2013	Publication
V1.2.1	September 2015	Publication
V1.3.1	March 2017	Publication
V1.4.1	August 2018	Publication
V1.5.1	January 2022	Publication
V1.5.2	July 2022	Publication